HELIX UNIVERSAL PROXY ADMINISTRATION GUIDE

Helix™ Universal Proxy version 9.0

RealNetworks, Inc.
PO Box 91123
Seattle, WA 98111-9223
U.S.A.

http://www.real.com
http://www.realnetworks.com

Printed in the United States of America.

CONTENTS

INTRODUCTION

Welcome to Helix™ Universal Proxy version 9.0, the most powerful caching proxy server available for streaming media. Helix Universal Proxy teams with media servers and players to optimize bandwidth and improve the playback experience. This manual will help you use and take full advantage of Helix Universal Proxy for real-time delivery of media files.

What is Helix?

Helix™ from RealNetworks is a universal digital media delivery platform. With industry-leading performance, integrated content distribution, advertising, user authentication, Web services support, and native delivery of RealMedia, Windows Media, QuickTime, and MPEG-4, Helix from RealNetworks is a robust digital media foundation that meets the needs of enterprises and networking service providers.

Audience for this Guide

This guide is intended for system administrators who will set up and manage Helix Universal Proxy.

Helix Universal Proxy Administration Guide is also available online at **http://service.real.com/help/library/index.html**.

How This Guide Is Organized

This guide contains the following chapters:

Chapter 1: New Features

If you're familiar with previous versions of proxy servers from RealNetworks, this chapter will give you a quick update on the new features found in Helix Universal Proxy.

Chapter 2: Overview

This chapter gives the “big picture” of how Helix Universal Proxy works.

Chapter 3: Installation and Quick Start

Find out how to install and start Helix Universal Proxy, and how to use the Web-based administration tool, Helix Administrator. Options for starting Helix Universal Proxy automatically, on different platforms are discussed as well as license information.

Chapter 4: Proxy Setup

This chapter discusses configuration options involving addresses, ports, and some differences between Helix Universal Proxy and Helix™ Universal Server. Most options are configured at installation and may need no changing.

Chapter 5: Client Configuration

This chapter describes how to set up RealOne Player and Windows Media Player to contact Helix Universal Proxy.

Chapter 6: Firewalls

If you are delivering content to users on the Internet, you’ll want to know how Helix Universal Proxy and other RealNetworks products interact with firewalls.

Chapter 7: Proxy Routing and Redundant Proxies

By employing several Helix Universal Proxys at once, you can funnel all streaming media Internet traffic through a single point. You can also create redundant network paths for your streaming media traffic.

Chapter 8: Multicasting

This chapter discusses multicasting, in which Helix Universal Proxy relays a single, live stream to multiple clients, rather than a separate stream to each client.

Chapter 9: Bandwidth Management

Helix Universal Proxy has several methods of managing the amount of bandwidth it uses. You can limit the amount of bandwidth in use at one time, and place a cap on the number of clients who can receive streaming media.

Chapter 10: Access Control

Learn how to limit which clients use your Helix Universal Proxy, based on their IP addresses.

Chapter 11: Authentication

Learn how to validate users attempting to access your Helix Universal Proxy with usernames and passwords.

Chapter 12: Proxy Monitor

To provide highest quality service, you'll want to keep track of how many clients are accessing your Helix Universal Proxy.

Chapter 13: Access and Error Logs

Helix Universal Proxy can report client behavior with a customizable degree of detail. Errors are reported in their own log, which can help you troubleshoot any problems that arise.

Chapter 14: Custom Logging

Helix Universal Proxy custom logging provides a way for you to create your own unique logging system using custom templates, or by using the built-in templates already provided.

Chapter 15: Troubleshooting

If something isn't working the way you expected, use this chapter as a resource to find your way.

Appendix A: Configuration File

This appendix presents a discussion on the basics of the Helix Universal Proxy configuration file, as well as XML syntax used in the file.

Appendix B: Address Space Bit Masks

This appendix explains how to identify a range of IP addresses by assigning a bit mask to a 32-Bit IP address. This is handy information for the access control and multicasting features.

Appendix C: Authentication Data Storage

Helix Universal Proxy comes with different methods for tracking authentication information, as described in this appendix. With this information you can set up your own authentication database.

Conventions Used in This Manual

This section explains some conventional terms and formats used throughout the book.

Terminology

Because this guide is designed for the Helix Universal Proxy administrators, the term "you" refers to the administrator.

RealNetworks clients, such as RealOne Player, or Windows Media Player are referred to generically as "clients". Where information applies specifically to the RealNetworks® RealOne Player, this is spelled out.

> **Note:** Although most clients currently in use are computers running RealPlayer or RealOne Player, RealNetworks also makes a software development kit (SDK) that enables other companies to develop their own players with which they can use to receive the various types of streamed data.

"Clips," "content," "media files," and "files" are used interchangeably to indicate the material that Helix Universal Proxy streams.

Typographical Conventions

The following table explains the typographic conventions used in this guide:

Notational Conventions

Convention	Meaning
`syntax`	This font is used for syntax of configuration files, URLs, or command-line instructions.
variables	Italic text represents variables. Substitute values appropriate for your system.
emphasis	Bold text is used for emphasis.

(Table Page 1 of 2)

Notational Conventions (continued)

Convention	Meaning
. . .	Ellipses indicate nonessential information omitted from examples.
[ ]	Square brackets indicate optional material. If you choose to use the material within the brackets, don't type the brackets themselves. An exception to this is in the access log, where statistics generated by the `ClientStats` variable are enclosed in regular brackets.

(Table Page 2 of 2)

Default Locations and Values

In all of the examples given in this book, it's assumed that you've installed Helix Universal Proxy in the default location for your operating system and that you're using default values for all settings. Of course, you can customize Helix Universal Proxy however you want to meet your specific needs. Default values are used here for clarity of illustration. On Windows-based platforms, the default installation directory is:

```
C:\Program Files\Real\Helix Proxy
```

Additional RealNetworks Resources

In addition to this guide, the following RealNetworks resources are available at: **http://service.real.com/help/library/index.html**

- Helix™ Universal Proxy Release Notes

  The release notes contain the very-latest information about Helix Universal Proxy. To view this information, click **Readme** in Helix Administrator.

- *Helix Universal Server Administration Guide*

  Information about Helix Universal Server, powerful software for streaming media content is covered in this basic reference. This guide explains how to set up, configure, and run Helix Universal Server to stream multimedia.

- Firewall Support

  This resource contains information on using our products with firewalls from several perspectives.

- General Information

You can read about Helix Universal Proxy special offers at:
http://www.realnetworks.com/products/proxy

- *Helix Universal Proxy Configuration File Reference*

  For those who prefer configuring Helix Universal Proxy by editing the configuration file directly, this reference is available at:
  http://www.realnetworks.com/resources/contentdelivery/gateway/config_variables.html

- *Helix Universal Server Configuration File Reference*

  For those who prefer configuring Helix Universal Server by editing the configuration file directly, this reference is available at:
  http://www.realnetworks.com/resources/contentdelivery/server/config_variables.html

CHAPTER

1

NEW FEATURES

Helix™ Universal Proxy version 9.0 is designed on a new architecture that facilitates greater extensibility and interoperability with third-party solutions. This chapter discusses features that have been added to the latest version of Helix Universal Proxy as well as upgrade issues.

New Features in Helix Universal Proxy

RTSP Cache Data Acquisition

Helix Universal Proxy now uses the RTSP protocol to transfer data from Helix™ Universal Server to its cache. Using RTSP to establish a cache acquisition connection (rather than the proprietary protocol MEI used in previous versions) removes the need for an organization to perform a special configuration of its firewall settings to work with Helix Universal Proxy. Additionally, since it's not HTTP caching it will not interfere with your system's web caching capability.

RTSP Splitting

Helix Universal Proxy now uses the RTSP protocol to request live splitting connections from Helix Universal Server. The proxy makes an RTSP control channel connection destined for the server on port 554 to request live broadcasts and to negotiate live packet transmission. Additionally this version of the proxy has an auto negotiation feature for live split broadcasts that first attempts UDP for live packet transmission and then TCP (if UDP is unavailable).

SureStream Aware Splitting

Teamed with Helix Universal Server, Helix Universal Proxy helps you conserve bandwidth when splitting a live RealAudio or RealVideo broadcast. With Surestream-aware splitting, this version of Helix Universal Proxy typically proxies only the bit rates requested by the client rather than sending multiple bit rate streams.

Windows Media

The Windows Media format can be streamed through this version of Helix Universal Proxy to Windows Media Player. Helix Universal Proxy proxies Windows Media format using Microsoft Media Services protocol (MMS).

MPEG

Working with Helix Universal Server, this version of Helix Universal Proxy supports MPEG 1 and MPEG 4.

- *MPEG-1:* Helix Universal Proxy delivers ISO/IEC 1172 compliant video and system bit streams. RealOne Player and QuickTime Player, for example, can play MPEG-1 streams. Helix Universal Proxy delivers MPEG-1 content with file extensions of `mpa`, `mpg`, `mpeg`, `mpv`, `mps`, `m2v`, `m1v`, and `mpe`.
- *MPEG-4:* Helix Universal Proxy supports hinted MPEG-4 content that uses the file extension `mp4`. It delivers ISMA/3GPP compliant bit streams, and you can view MPEG-4 bit streams using any ISMA/3GGP compliant client, such as RealOne Player and RealOne Mobile Player.

  Note: Helix Universal Proxy delivers MPEG files on-demand. It does not currently support live MPEG broadcasting, except with the MP3 format. But if the origin Helix Universal Server is simulating a live broadcast using the server feature SLTA, Helix Universal Proxy can deliver any supported, prerecorded MPEG clip.

RealMedia Variable Bit Rate

Teamed with Helix Universal Server, this version of Helix Universal Proxy delivers RealMedia Variable Bit Rate (.rmvb) video format by proxy cache in addition to delivery by pass-through mode.

Custom Logging

Custom logging is a more flexible system for generating reports. This type of logging is based on templates that define what information is captured, when and how often information is captured, and how it is delivered. You can create your own templates or use the default templates. For more information, see Chapter 14, "Custom Logging".

Redundant Proxies

The redundant proxies feature enables you to add another level of redundancy to the delivery of your streaming media content. If an RTSP connection between RealOne Player and Helix Universal Proxy breaks, by default the RealOne Player attempts to reconnect to the same Helix Universal Proxy. However, in this version of Helix Universal Proxy, if you have identified an alternate proxy, RealOne Player attempts to connect to the alternate proxy instead. For more information see, "Working With Redundant Proxies" on page 80.

Upgrade Issues

This section explains issues about upgrading to Helix Universal Proxy.

Compatibility with Server Versions

Everything that you use Helix Universal Proxy for performs seamlessly with Helix Universal Server and all later versions of RealSystem Server. For more details, refer to the following table.

Helix Universal Proxy Compatibility with Server Versions

Helix Universal Proxy Feature	Helix Universal Server 9.0	RealSystem Server Version Number 8.x, 7.0	G2 (6.0)	5.0 and earlier
Pass-through	**yes**	**yes**	**yes**	**yes**
Pull splitting	**yes** (RTSP only)	**yes** (RTSP only)	**yes** (RTSP only)	no
Caching	**yes**	**yes**	**yes**	no

Tip: To use pull splitting with RealSystem Server version 8 you need to modify the Helix Universal Proxy configuration file, `rmproxy.cfg`. Refer to "Pull splitting with RealSystem Server version 8" on page 45.

Default Installation Directory

On Windows, Helix Universal Proxy installs into the following default location, which differs from the installation paths for previous versions of RealSystem Proxy:

```
C:\Program Files\Real\Helix Proxy
```

If you choose the default location, you may need to move logs and other files to the new directory tree, as described in "Upgrading in a Different Directory" on page 27.

CHAPTER

2

OVERVIEW

Designed to securely re-serve streaming media, Helix Universal Proxy delivers an impressive array of media to the broadest range of media players. This chapter introduces you to Helix Universal Proxy concepts and features.

Understanding Helix Universal Proxy

Helix Universal Proxy is software you install on a network or ISP gateway that gathers and handles client requests for media streamed from Helix™ Universal Server. Helix Universal Proxy reduces network traffic by eliminating redundant requests for streaming media.

The proxy provides four main benefits:

- reduces bandwidth consumption by eliminating redundant data transmissions
- improves quality of user experience by distributing streaming media close to the user
- provides mechanisms for controlling inbound and outbound bandwidth parameters, thus securing bandwidth for other applications
- masks the IP addresses of the client software

Media Types

Helix Universal Proxy can proxy every media type that the origin Helix Universal Server can serve. Helix Universal Server streams on-demand clips and broadcasts live events in more media formats than any other media server. Depending on its license type, Helix Universal Server can serve the file formats listed below. Although not exhaustive, the following list represents the major media formats available with Helix Universal Server and Helix Universal Proxy,

which can deliver additional formats through plug-ins created by third-party developers.

RealNetworks:	RealAudio (.rm), RealVideo (.rm), RealPix (.rp), RealText (.rt), RealMedia Variable-Bit Rate (.rmvb)
Macromedia:	Flash 4 (.swf)
Microsoft:	Windows Media (.asf, .wma, .wmv)
Apple:	QuickTime (.mov)
Other:	MPEG 1, MPEG 4 (.mpg, .mpeg), MP3 (.mp3), AU (.au), AIFF (.aif, .ief), WAV (.wav), SMIL (.smi, .smil)
Image Formats	GIF (.gif), JPEG (.jpg, jpeg), PNG (.png)

Working with Helix Universal Server, Helix Universal Proxy can deliver the same media formats on any platform, including Windows and many UNIX variants. This allows you to stream any supported format using the operating system of your choice. Helix Universal Proxys running on different operating systems are completely interoperable, allowing you to place multiple proxies and servers in a heterogeneous network environment.

The specific versions of media formats and media players supported by Helix Universal Server and Helix Universal Proxy are subject to change. Check **http://www.realnetworks.com/resources** for the latest information.

How Helix Universal Proxy Delivers Media

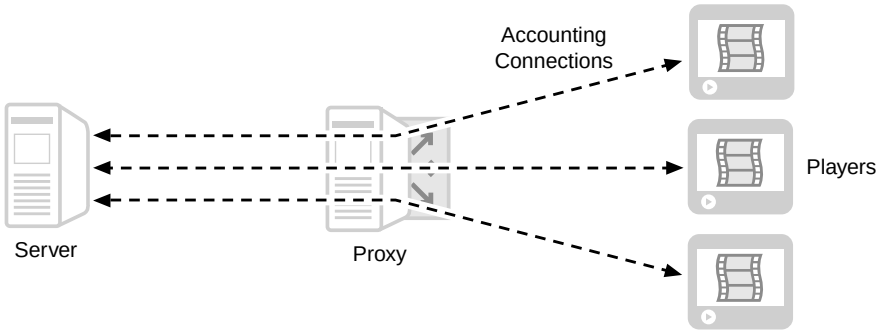
The first step in the process happens when clients, such as RealOne Player or Windows Media Player request streamed media files through Helix Universal Proxy.

Helix Universal Proxy forwards the requests on behalf of clients to the Helix Universal Server where the requested streamed media files are stored (called the “origin Helix Universal Server”).

Helix Universal Server verifies the file’s existence, and that the clients are authorized through IP addresses or content authentication. If the server denies the request, it does not stream the requested file; Helix Universal Proxy complies with the denial. Clients receive an applicable error message.

This initial transaction, in which Helix Universal Server examines and authorizes individual client requests, is called an “accounting connection”, as shown in the following diagram.

Establishing the Accounting Connection with Helix Universal Proxy and Helix Universal Server

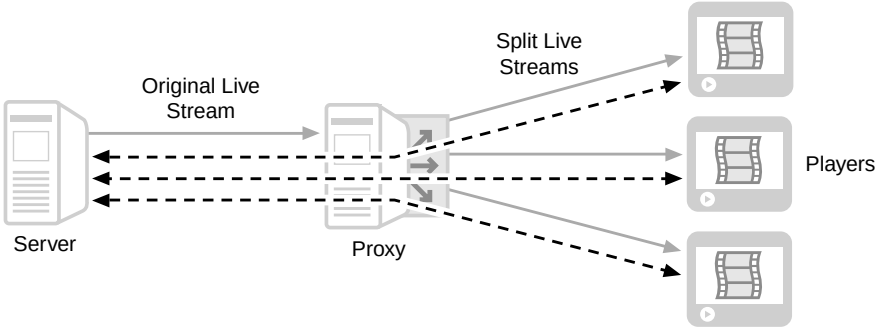


Depending on the nature of the streaming media, Helix Universal Proxy uses different features to deliver the content to the client.

Live Stream Delivery

If the stream is live, Helix Universal Proxy replicates the live stream for each client requesting the stream. The origin Helix Universal Server sends only a single stream to Helix Universal Proxy.

Helix Universal Proxy Replicating Live Content



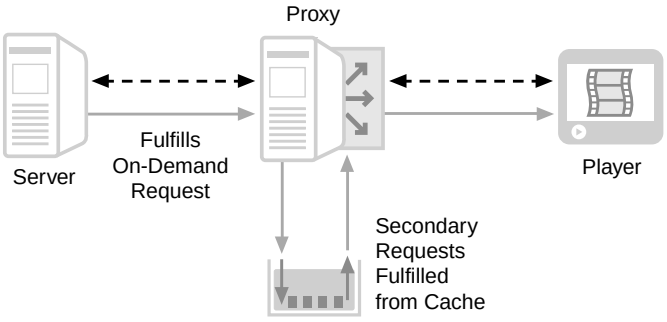
If the live stream is not available for replicating, Helix Universal Proxy makes a separate data request to the Helix Universal Server for each client. This is known as the pass-through feature, as shown in "Pass-through Mode (for Live and On-Demand Streams)".

On-Demand Content Delivery

If the stream is on-demand, Helix Universal Proxy first tries to fill the request from the media cache.

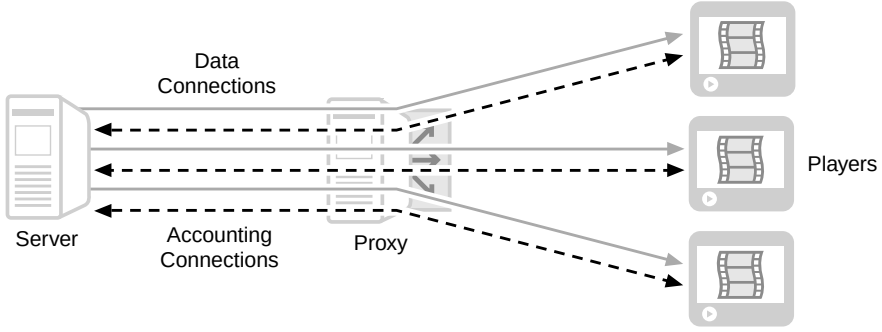
If the content is not yet stored in the cache, Helix Universal Proxy will pull the content from the origin Helix Universal Server, simultaneously serving the client and filling the cache.

Helix Universal Proxy Streaming On-Demand Content from the Cache



If the stream is on-demand, and the clip is not cachable, Helix Universal Proxy delivers media by the pass-through feature. The proxy passes a data stream for each client that requested it, as shown in the following diagram.

Helix Universal Proxy Streaming On-Demand Content (No Media Cache in Use)



A media cache file lowers network traffic by reducing the number of connections to the origin of the requested material, and improves quality by distributing the streaming content closer to the user. Clients receive improved quality of service because media streams travel a shorter distance from the cache to clients, reducing the possibility of network congestion, latency or packet loss.

Helix Universal Proxy Features

Helix Universal Proxy has three different ways of sending clips to clients. Helix Universal Proxy automatically chooses the most efficient feature possible, based on the type of content requested and the network configuration. The three methods are:

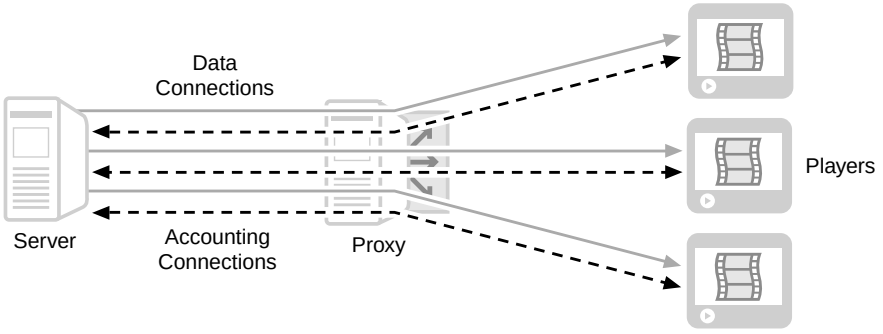
- **Pass-through**—No bandwidth conservation is in effect, but all streaming media (both on-demand and live) requests go through Helix Universal Proxy.
- **Pull Splitting**—For live requests, Helix Universal Proxy "shares" the stream among the clients who request it.
- **Cache**—For on-demand requests, Helix Universal Proxy securely stores the streaming media data for later viewing by other clients.

In addition, you can configure pull splitting to transmit to clients using multicast. Regardless of the feature in use, Helix Universal Proxy always opens an accounting connection between the client and the origin Helix Universal Server.

Pass-through

This is Helix Universal Proxy's simplest method of operation. In addition to the usual accounting connection opened between the client and the origin Helix Universal Server, Helix Universal Proxy creates a data connection for each client. No bandwidth conservation is realized.

Pass-through Mode (for Live and On-Demand Streams)



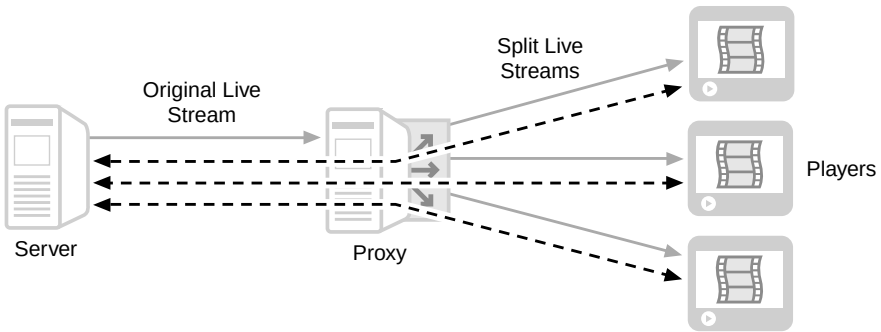
Pull Splitting

Pull splitting conserves bandwidth for live material by replicating a single live stream from an origin Helix Universal Server. The first time a client requests a particular stream, Helix Universal Proxy contacts the origin server on the client's behalf and then sends the stream to the client. The second client to request the same live stream will receive it directly from Helix Universal Proxy, and Helix Universal Proxy will not have to obtain another stream from the origin Helix Universal Server.

The advantage to the client is that the material is delivered from a nearby Helix Universal Proxy. As long as the quality of reception for the single split channel between Helix Universal Proxy and the origin Helix Universal Server is sustained, clients will receive a high-quality live stream as well.

Additionally, Helix Universal Proxy can deliver a live, pull-split stream using multicast, if available on the network.

Pull Splitting Mode (for Live Streams)



Cache

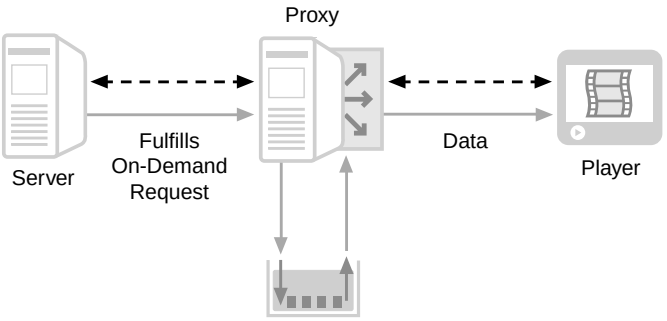
Cache software stores on-demand content from origin Helix Universal Servers. Since cached files are securely stored and cannot be accessed directly, Helix Universal Proxy interfaces with the cache to redistribute the stored media to clients.

When caching is enabled, the media cache acquires and stores media files requested by the first client. When a second client makes a request for a stream, Helix Universal Proxy checks with the cache to see if a stored version is already present. To ensure that the stored version is the most up-to-date version available, Helix Universal Proxy checks with the origin Helix Universal Server to see if a newer version exists. After determining that the stored copy is

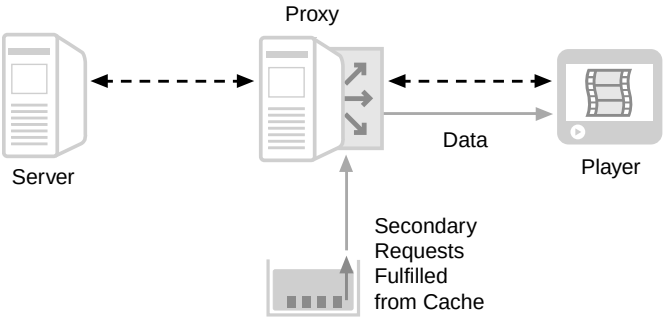
the latest version, Helix Universal Proxy streams the stored copy to the second client, and to subsequent clients that request the same material.

On-demand material streamed by RealSystem Server 7.0 or later can be cached. Otherwise, they are delivered by the pass-through feature. Live material is handled in the most efficient mode suitable—pull splitting or pass-through.

Filling the Media Cache with On-Demand Clips



Serving On-Demand Clips from the Cache



Should the media in the cache become impaired in some way, the stream halts and clients receive an error message. If the accounting connection between the client and the origin Helix Universal Server is interrupted, Helix Universal Proxy terminates the stream, and the client receives an error message.

If an origin Helix Universal Server has been configured to prevent caching, Helix Universal Proxy will use the pass-through feature to deliver content to clients, without caching the media. When Helix Universal Server is installed, all its streams are cachable by default. Since Helix Universal Servers can save on bandwidth costs if caching is allowed, operators are encouraged to leave all content cachable.

Requirements for Each Helix Universal Proxy Feature

The following table outlines the configuration requirements for each aspect of Helix Universal Proxy operation. In addition, Helix Universal Proxy can be configured to use multicasting (where available) for those live clips delivered in pull splitting mode. For more information, see Chapter 8, "Multicasting".

Requirements for Each Feature

Feature	Special Helix Universal Proxy Configuration	Your Network Requirements (assumes Helix Universal Proxy is running)	Origin Helix Universal Server Requirements
Pass-through	None.	None.	Broadcasting live and/or on-demand content.
Pull splitting	None. Helix Universal Proxy is configured to do pull splitting by default.	Network allows UDP transport between Helix Universal Proxy and Helix Universal Server. If UDP is unavailable, Helix Universal Proxy automatically attempts TCP.	Broadcasting live content. Configured to allow pull splitting, with default values. (Default configuration of Helix Universal Server.)
Caching	None. Helix Universal Proxy is configured to cache by default.	None.	Has on-demand content, and is configured to accept requests from caches. (Default configuration of Helix Universal Server.)
Multicasting (back-channel)	Configured to use multicast address range. Helix Universal Proxy uses pull splitting to deliver clips.	Clients and routers are multicast-enabled.	Broadcasting live content.

Additional Features

Helix Universal Proxy contains additional features that make it easy to configure, administer, and maintain.

Helix Administrator

Helix Administrator is a secure HTML-based interface for customizing Helix Universal Proxy features. You can access the Administrator with a Java-enabled browser anywhere on your network. The latest version of your Web browser is recommended for browsing Helix Administrator. Refer to "Using Helix

Administrator" for more information. Additionally, see Chapter 4, "Proxy Setup" for instructions on customizing Helix Universal Proxy.

> **Tip:** In this guide, "Helix Administrator" with an uppercase "A" refers to this HTML-based tool, whereas "RealNetworks administrator" with a lowercase "a" refers to the person who configures and runs Helix Universal Proxy.

Changes you make using Helix Administrator are stored in the Helix Universal Proxy configuration file. This text file is based on XML (Extensible Markup Language) that you can edit directly. Because the structure of this file is complex, Helix Administrator is the recommended tool for making changes. Appendix A discusses the configuration file.

Limiting Network Traffic

To limit the amount of bandwidth used by Helix Universal Proxy, several features allow you to restrict the number of requests or amount of bandwidth it uses. Clients that attempt to contact Helix Universal Servers after Helix Universal Proxy's limits have been reached, receive an error message.

> **For More Information:** See Chapter 9, "Bandwidth Management".

Proxy Routing

For organizations that use strict rules to regulate network traffic, proxy routing allows you to further control streaming media traffic. With this feature, you can configure Helix Universal Proxy to direct its clients' requests to yet another Helix Universal Proxy, thereby conserving bandwidth across the WAN.

> **For More Information:** See Chapter 7, "Proxy Routing and Redundant Proxies".

Monitoring Helix Universal Proxy in Real Time

Helix Administrator includes a Monitor which dynamically displays the status of your Helix Universal Proxy.

> **For More Information:** Refer to Chapter 12, "Proxy Monitor".

Tracking Helix Universal Proxy Activity

Helix Universal Proxy records information in the access log about all clips it has served. Errors are noted in the error log. You can also design your own custom logs based on proxy activity.

Access logs are similar in format to Helix Universal Server logs, but include additional information about the address of the origin Helix Universal Server and the Helix Universal Proxy operational mode (pull splitting, caching, and so on). Helix Universal Proxy error logs use the same format as Helix Universal Server error logs. Content and format of custom logs depend on your instructions to Helix Universal Proxy.

Log files on the origin Helix Universal Server show that a Helix Universal Proxy is in use in addition to client data.

> **For More Information:** Access and error log information is described in depth in Chapter 13, "Access and Error Logs". Refer to Chapter 14, "Custom Logging" to learn how to implement that feature.

Working with Clients

In order for Helix Universal Proxy to fill requests for media, you will need to arrange for clients (such as RealOne Player and Windows Media Player) to send their requests to Helix Universal Proxy.

There are two ways you can do this:

- Configure clients to directly contact Helix Universal Proxy with their streaming media requests. You can send instructions for doing this to users. Refer to Chapter 5, "Client Configuration".
- Configure Helix Universal Proxy to intercept client requests. This does not require any special client configuration, but it does require the use of software or hardware which routes TCP traffic by destination port (such as a layer-4 switch). Consult your switch manufacturer's documentation for details. Additionally, refer to the Helix Universal Proxy Readme document for more information, at **http://service.real.com/help/library/guides/proxy2/readme.html**

Interaction with Helix Universal Server

This section describes what happens on the origin Helix Universal Server when Helix Universal Proxy forwards a client request.

> **For More Information:** If you plan to manage both Helix Universal Proxy and Helix Universal Server, also refer to the section "Administering Both Helix Universal Proxy and Helix Universal Server".

Controlling Client Access

Each time it receives a request, Helix Universal Server determines whether it can allow a particular client to receive streams, based on the number of available streams and bandwidth. In addition, Helix Universal Server can be configured to require a user name and password for certain material. If the requested material requires a password, the user will be prompted for the password. In this case, Helix Universal Server does not begin streaming until it receives the correct password.

Only after Helix Universal Server has authorized the client's request will Helix Universal Server begin streaming. Restrictions imposed by the origin Helix Universal Server's administrator on client access are always honored by Helix Universal Proxy. The same is true when a cache is in use—Helix Universal Proxy waits for Helix Universal Server approval of each request before streaming it from the cache.

Denying Client Access

An origin Helix Universal Server may deny a request for the following reasons:

- The requested material is secured, and the user does not have permission to access it
- Helix Universal Server can restrict access according to IP address, and the client's IP address or the Helix Universal Proxy's IP address is on the restricted access list
- No more connections are available on the origin Helix Universal Server. The number of connections is governed by the license, and can be further limited by the person managing the server.

The client receives a message if it is denied access for any reason.

Tracking Activity

The origin Helix Universal Server can differentiate whether a request was made using Helix Universal Proxy or made directly by any client. Information about quality of service is logged in the access log, just as it is for any other type of connection. Information about quality of service comes from the accounting connection.

Cache Requests

Helix Universal Proxy only streams media from the cache after opening an accounting connection to the origin Helix Universal Server. If the accounting connection cannot be established, or if it is disrupted, proxy will not stream from the cache to the client.

Helix Universal Proxy cannot cache content which an origin Helix Universal Server administrator has configured as non-cacheable. Instead, it will use pass-through mode to deliver the material to the client.

When Helix Universal Proxy Will Not Conserve Bandwidth

Under the following circumstances, Helix Universal Proxy will be unable to conserve bandwidth:

- If the origin Helix Universal Server is configured to only allow caching on some files, or not at all. You have no control over this. (For example, a server administrator might prevent frequently updated material, such as advertisements, from being cached.)
- If the origin Helix Universal Server does not allow pull splitting, this feature is disabled and Helix Universal Proxy will deliver media by pass-through mode.

In all cases, however, using Helix Universal Proxy on your network serves to collect all streaming media traffic at a single point, so that you can better monitor activity and maintain security.

Protocols, Transports, and Packet Formats

Helix Universal Proxy handles client requests and proxies Helix Universal Server streams by using the Real Time Streaming Protocol (RTSP), an Internet standard control protocol for streaming multimedia, and PNA, the

RealNetworks legacy protocol. Additionally, Helix Universal Proxy can use MMS to stream Windows Media. Although Helix Universal Server can stream through HTTP, Helix Universal Proxy is not an HTTP protocol proxy and thus does not handle any streaming media requests made through HTTP between clients and an origin Helix Universal Server.

Helix Universal Proxy works with connecting clients such as RealOne Player and Windows Media Player to determine the best transport to use for a given stream: IP multicast (for live broadcasts), or UDP and TCP (for both live and on-demand content).

Data types streamed by Helix Universal Server and Helix Universal Proxy use two primary packet formats: RDT, a proprietary packet format native to RealNetworks, and RTP, an Internet standard data type packet format.

The following table outlines the protocols, transports, and packet formats supported by Helix Universal Proxy.

Supported Protocols and Data Packet Formats

Control Protocol	Control Transport	Data Packet Format	Data Packet Transport	Supported by Helix Universal Proxy?
RTSP	TCP TCP	RDT (RealNetworks) RTP	IP multicast, UDP, TCP	Yes
PNA (RealSystem Server 5.0 and earlier)	TCP TCP	RDT (RealNetworks) RTP	UDP, TCP	Yes
MMS	TCP	—	UDP, TCP	Yes
HTTP (Streaming)	TCP	—	—	No
HTTP (Cloaking)	TCP	RDT (RealNetworks), RTP	TCP	

For More Information: For details on the control transports and data packet transports allowed on each port, see Chapter 6, “Firewalls”.

CHAPTER

3

INSTALLATION AND QUICK START

This chapter explains how to install Helix Universal Proxy on Windows and UNIX platforms. It also introduces you to Helix Administrator, the Web-based tool for configuring Helix Universal Proxy. As soon as you start Helix Universal Proxy, it is ready to stream media, and the last section walks you through processes for configuring a client to use your Helix Universal Proxy.

Installing Helix Universal Proxy

To install Helix Universal Proxy, you need a binary installation file and a license file, which enables Helix Universal Proxy features. Although you can install Helix Universal Proxy without the license file, Helix Universal Proxy will not operate until you have obtained a valid license file. License files are delivered by e-mail after you download or purchase Helix Universal Proxy.

> **Note:** If you're installing on UNIX, you have to log in as `root` to perform a default installation because the default value for the RTSP port is lower than 1024.

➤ To install Helix Universal Proxy:

1. Launch the binary setup file you downloaded. If you have a Helix Universal Proxy installation CD, open the folder named for the operating system you are using, and execute the setup file.
2. Read the installation recommendations and press **Enter**.
3. Enter the path to the license file you received from RealNetworks, and press **Enter**. The installation process copies the license file to the `License` subdirectory under the main Helix Universal Proxy directory. On startup, Helix Universal Proxy reads that copy of the license.
4. Read the end-user license agreement, signifying your agreement to its terms and conditions by pressing **Enter**.

5. Enter a path where you want to install Helix Universal Proxy, or accept the default path on Windows. Examples in this guide assume that you've chosen the default path.

   Note: On Windows, the default installation path for Helix Universal Proxy differs from previous versions of RealSystem Proxy. For more information, see "Upgrading in a Different Directory" on page 27.

6. Enter a user name and password, and then confirm your password by entering it again. Your user name and password are required to access various Helix Universal Proxy features, such as Helix Administrator. Choose a password that is difficult to guess, and that includes both letters and numbers. The password is case-sensitive.

7. In the next set of screens, you define ports that Helix Universal Proxy uses for the PNA, RTSP, HTTP, and MMS protocols, as well as the port used by Helix Administrator. RealNetworks recommends accepting the default ports, unless those port values will cause conflicts with other applications. Note the following:

   - You can change the port settings later, as described in "Defining Communications Ports" on page 46.
   - You will need the Admin port number to connect to Helix Administrator from a Web browser. As a security feature, the installer randomly generates this port number. RealNetworks recommends that you accept the default, but you can change the port value if you wish, or you know that the selected value will conflict with another port assignment. In either case, remember the port number, or record it in a secure location.

8. On Windows, the default installation sets up Helix Universal Proxy as a service. This is optional - you can prevent this by clearing the **Run as NT Service** box. If you choose, you can later set up Helix Universal Proxy to run as a service, as described in "Configuring Helix Universal Proxy as a Windows Service" on page 31.

9. In the final confirmation screen, review and accept the installation information to complete the installation process.

Upgrading in a Different Directory

If you are upgrading, and you install Helix Universal Proxy in a path that differs from that of your previous RealSystem Proxy, move some of your existing files from the previous installation directory to the new directory after the installation. You'll need to do this, for example, if you chose the default installation path on Windows:

```
C:\Program Files\Real\Helix Proxy
```

Optionally, you'll need to move files in the `Logs` directory. If you are using authentication, you'll also need to move the files described in Appendix C.

If you plan to use a configuration file from an earlier version of RealSystem Proxy, you need to edit the configuration information manually to reflect the new installation directory. Look for the variables that list full paths, and change their values accordingly.

> **Warning!** Because editing the configuration file with a text editor can potentially disable Helix Universal Proxy, be sure to read Appendix A before attempting modifications.

Reinstalling Helix Universal Proxy in the Same Directory

Reinstallation is generally not necessary, but if needed, you can reinstall Helix Universal Proxy by repeating the installation procedure described in "Installing Helix Universal Proxy" on page 25. A reinstallation does not affect proxy cache, but it resets your Helix Universal Proxy configuration values to their defaults. If you tailored your system configuration after the initial installation, the following tips allow you to retain your data and make your reinstallation process smoother:

- Back up the configuration file (`rmproxy.cfg`) to preserve the configuration information. After the reinstallation, replace the file created by the installer with your backup.
- Back up any authentication databases (`adm_b_db`, `con_r_db`, and so on) that you've revised or added. This step is necessary only if you've added more users and passwords for authentication than those added during installation. Appendix C explains authentication databases.
- Note the value of the Admin port (**Proxy Setup>Ports**). If you bookmarked Helix Administrator in your browser, specify the same Admin port during the reinstallation to keep the bookmark functional.

- A reinstallation does not affect cache files, access logs, or error logs. It is therefore not necessary to back up these files before reinstallation. These files reside in the `Cache` and `Logs` subdirectories of the main installation directory.

Running Helix Universal Proxy

This section describes how to start and stop Helix Universal Proxy on Windows and Unix. It lists command line options that you can use when starting Helix Universal Proxy manually. Additionally, it explains how to configure Helix Universal Proxy as a Windows service if you did not select that option during installation.

Starting Helix Universal Proxy

When you start Helix Universal Proxy manually, you can select which configuration file you want to use. You can also specify command line options on both Windows and UNIX. As described in "Restarting Helix Universal Proxy" on page 37, you can use Helix Administrator to restart Helix Universal Proxy following a configuration change.

Starting on Windows

In its default Windows installation, Helix Universal Proxy is set up as service named "Helix Universal Proxy." In this case, Helix Universal Proxy always runs in the background, and you do not need to start it. If you did not install Helix Universal Proxy as a Windows service, you can start it from the **Start** menu, a desktop icon, or the command line.

Starting Up from the Start Menu

From the **Start** menu, select **Programs>Helix Proxy>Helix Proxy**. Helix Universal Proxy loads the default configuration file, `rmproxy.cfg`.

Starting Up from the Command Line

From the **Start** menu, open the command prompt. Navigate to the Helix Universal Proxy folder, and enter the following command to start Helix Universal Proxy with its default configuration file. You can use a different configuration file if you wish:

```
Bin\rmproxy rmproxy.cfg
```

Starting on UNIX

You can start Helix Universal Proxy as an application or as a background process. The following procedure uses the default configuration file (`rmproxy.cfg`), but you can specify a different file.

> **Note:** If you performed a default installation of Helix Universal Proxy, the RTSP port is set lower than 1024, requiring the user who starts Helix Universal Proxy to log in as `root`.

➤ To start Helix Universal Proxy on UNIX:

1. Start any command shell.
2. Navigate to the main Helix Universal Proxy installation directory.

   > **Warning!** If you do not start Helix Universal Proxy from its `Bin` directory, it cannot understand the relative paths in the configuration file.

3. Choose one of the following options:
   a. Start Helix Universal Proxy in the background with the following command:

      ```
      Bin/rmproxy rmproxy.cfg &
      ```

   b. Start Helix Universal Proxy as an application:

      ```
      Bin/rmproxy rmproxy.cfg
      ```

   c. Optionally, you can limit the amount of memory that Helix Universal Proxy uses by including the `-m` parameter, where the number after `-m` specifies the amount of memory in Megabytes (must be greater than 32). The following example starts Helix Universal Proxy as an application:

      ```
      Bin/rmproxy rmproxy.cfg -m 512
      ```

      The next example starts Helix Universal Proxy as a background process:

      ```
      Bin/rmproxy rmproxy.cfg -m 512 &
      ```

      > **Note:** If the Helix Universal Proxy machine is dedicated to running Helix Universal Proxy, RealNetworks recommends that you allocate 75% of the available system memory for Helix Universal Proxy's use.

Process ID (PID)

Helix Universal Proxy creates a text file that records the current value of the process ID of the parent Helix Universal Proxy process, `rmproxy`. The file is stored in the directory indicated by the `PidPath` variable, and is named `rmproxy.pid` at installation. If `PidPath` is omitted from the configuration file, Helix Universal Proxy stores the information in the directory specified by the `LogPath` variable.

Using Command Line Options

On both Windows and UNIX, you can include options when starting Helix Universal Proxy from the command line. You list options after the `rmproxy` executable name, preceding each option with one or two hyphens as shown here:

```
Bin/rmproxy --rss 60 rmproxy.cfg
```

Command line options have both short names and long names, as summarized in the following table. Additional, Windows-only command line options are described in "Configuring Helix Universal Proxy as a Windows Service" on page 31.

Command Line Options on Windows and UNIX

Short Name	Long Name	Function
`-v`	`--version`	Print version number and exit.
`-h`	`--help`	Print command line help and exit.
`--out <file>`	`--output-file <file>`	Redirect console output to file.
`--rss [n]`	`--report-server-stats [n]`	Report server statistics every *n* seconds. The default is 60 seconds.

Stopping Helix Universal Proxy

It's generally not necessary to stop Helix Universal Proxy when it's running. If you make configuration changes that require a restart, you can restart through Helix Administrator, as described in "Restarting Helix Universal Proxy" on page 37.

Shutting Down on Windows

If Helix Universal Proxy was started as a Windows service, stop it through the **Services** control panel. Give the **Start>Settings>Control Panel>Administrative**

Tools command and double-click **Services**. Locate Helix Universal Proxy on the list (your service name may be different), highlight it, and click **Stop**.

If you started Helix Universal Proxy manually, switch to the command window and press **Ctrl+c**. You can also use the Task Manager (**Ctrl+Shift+Esc**) to end the Helix Universal Proxy task.

Shutting Down on UNIX

To stop Helix Universal Proxy on UNIX, obtain the parent process identification number, and then issue the `kill` command with that process number. The process ID is stored in the `rmproxy.pid` file, which is usually kept in the `Logs` directory. (The `PIDPath` variable in the configuration file specifies this location.) You can perform both actions with one command. From the command line, navigate to the directory that contains the Helix Universal Proxy PID file, and type the following, where *pidfile* is the name of the `PID` file:

`kill 'cat` *pidfile*`'`

Configuring Helix Universal Proxy as a Windows Service

If you did not set up Helix Universal Proxy to run as a Windows service during installation, you can do so at any time by following the procedure below on a Windows NT, or Windows 2000 machine.

➤ To set up Helix Universal Proxy as a service:

1. Stop Helix Universal Proxy.
2. From the **Start** menu, open the command prompt and navigate to the Helix Universal Proxy `Bin` directory.
3. Import the configuration file you want to use into a specific key in the Windows NT registry by typing the following:

   `rmproxy.exe -import[:`*key*`]` *configuration_file*

   using the following values:

key	The Windows NT registry key name you want to use. If you omit it, the default name `Config` is substituted.
configuration_file	The path and file name of the configuration file to import. The configuration file must use absolute paths for variables such as BasePath. Helix Universal Proxy does not recognize relative paths while running as a service.

   For example, the following command:

```
rmproxy.exe -import:Proxy1 ..\rmproxy.cfg
```

imports all of the values in the `rmproxy.cfg` file into the following key of the Windows registry:

```
HKEY_CLASSES_ROOT\Software\RealNetworks\Helix Proxy\9.0\Proxy1
```

Note that you can then start Helix Universal Proxy using this configuration by typing the following at a command line:

```
rmproxy.exe registry:Proxy1
```

4. Install the service by typing the following command at the command prompt:

   `rmproxy.exe -install[:`*`ServiceName`*`] "`*`parameters`*`"`

   using the following variables:

ServiceName	The name that will appear in the **Services** dialog box. If you omit *ServiceName*, `Helix Universal Proxy` is used.
parameters	Either the name of the configuration file, or the Windows registry and key name, as entered in Step 3. The format of the Windows NT registry and key name is registry:key. Any command line parameters can be used.

   Note: The quotation marks surrounding *parameters* are required. In addition, you must supply the path to the configuration file. Helix Universal Proxy may not start if it cannot find the configuration file.

   The next time you start Helix Universal Proxy from the Services dialog, it will use the settings specified in *parameters*, and will be configured to start automatically. For example, the following command:

   ```
   rmproxy.exe -install:RMLocal "registry:Proxy1"
   ```

   installs Helix Universal Proxy with the service name **RMLocal**, and uses the settings in the `Proxy1` key.

5. Start the service. In the Services control panel, select the name you used for *ServiceName*, and click **Start**.

Removing Helix Universal Proxy from the Services List

At a command prompt, type the following:

`rmproxy.exe -remove[:`*`ServiceName`*`]`

in which *ServiceName* is the optional name of the service. If you omitted a service name when you installed the service, you can omit it here, and Helix Universal Proxy will use Helix Proxy.

Running Multiple Helix Universal Proxys on One Windows NT System

You can have configuration files with different names for different configurations of a single Helix Universal Proxy, or use different names for different Helix Universal Proxy installations.

You can load configuration files into separate registry keys. Then, run Helix Universal Proxy as a service, one for each configuration file you loaded.

➤ To import a configuration file into a specific key in the registry:

1. Follow the instructions in Step 3 of "Configuring Helix Universal Proxy as a Windows Service".
2. Start Helix Universal Proxy by typing the following:

   `rmproxy.exe registry:`*key*

   where:

   key is name you want to use for the configuration. Helix Universal Proxy places the configuration information in `HKEY_CLASSES_ROOT\Software\RealNetworks\Helix Proxy\Key`.

   In the example from Step 3 of "Configuring Helix Universal Proxy as a Windows Service", in which the configuration settings are loaded into the "Proxy1" key, the full key name would be `HKEY_CLASSES_ROOT\Software\RealNetworks\Helix Proxy\9.0\Proxy1`.

Using Helix Administrator

Helix Administrator is Helix Universal Proxy's HTML-based interface. It allows you to modify and manage Helix Universal Proxy from anywhere on your network using a Web browser.

> **Tip:** In this guide, "Helix Administrator" with an uppercase "A" refers to this HTML-based tool, whereas "RealNetworks administrator" with a lowercase "a" refers to the person who configures and runs Helix Universal Proxy.

Starting Helix Administrator

To start Helix Administrator, you need to know the port number it uses, as well as the user name and password selected during Helix Universal Proxy installation. The password selected during installation is stored in the `MonitorPassword` variable of the configuration file. For background on the configuration file, see Appendix A.

➤ To start Helix Administrator:

1. Start Helix Universal Proxy. (See the section "Starting Helix Universal Proxy" for instructions).
2. Click the browser shortcut created by the Helix Universal Proxy installer, or use the following instructions:

   In a browser, use the following syntax:

   `http://`*`proxy.example.com`*`:`*`AdminPort`*`/admin/index.html`

   where:

   proxy is the name of the machine on which Helix Universal Proxy is installed.

   example.com is the name of the domain in which Helix Universal Proxy exists.

   Optionally, rather than typing the name and domain of the system on which Helix Universal Proxy is installed, you can use the IP address.

   AdminPort is the port which Helix Administrator uses to connect to Helix Universal Proxy. You are asked for a port number during setup. Use that port number here.

   If your browser is on the same computer as Helix Universal Proxy, you can typically use the localhost address (be sure to substitute your port number for *AdminPort)*:

   `http://localhost:`*`AdminPort`*`/admin/index.html`

   The following command also works on the same computer:

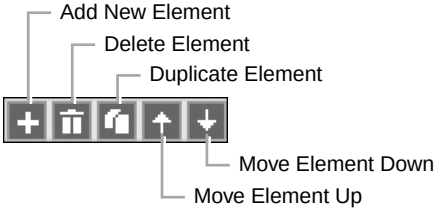
   `http://127.0.0.1:`*`AdminPort`*`/admin/index.html`
3. Enter the user name and password chosen during installation. The password is case-sensitive.
4. Click **OK** to start Helix Administrator.

Tip: You can create additional user names and passwords to let other people access Helix Administrator. For more information, see "Authenticating Helix Administrator Users" on page 105.

Navigating the Interface

Helix Administrator consists of HTML pages you use to configure Helix Universal Proxy. The left frame groups features into functional areas, as described below. Pages that display in the right pane typically consist of forms that include fields and pull-down lists. In pages that define multiple elements, you can use the control icons shown in the following illustration.

Helix Administrator Controls



Tip: If you are familiar with previous versions of RealSystem Administrator, note that you no longer have to click an **Edit** button to update an element definition. You simply enter the element information in the fields, and click **Apply** at the bottom of the page when you are finished.

Helix Administrator Sections

Helix Administrator's left-hand navigation pane groups Helix Universal Proxy features under functional areas such as **Security**. Click the name of a functional area to expand or collapse the list of features it contains. The following tables summarize all features, and point you to the sections of this guide that explain each feature.

Proxy Setup

The proxy setup features let you configure the basic functions of Helix Universal Proxy. Many of these features are preconfigured at installation.

Proxy Setup Features

Feature	Function	Reference
Ports	Define ports for communications protocols.	page 46
IP Binding	Select IP addresses Helix Universal Proxy uses.	page 47
Bandwidth Management	Limit the amount of bandwidth Helix Universal Proxy uses.	page 91
Proxy Routing	Setup proxy chains to other Helix Universal Proxys.	page 75
Redundant Proxies	Define failover proxies for streaming delivery.	page 80
Cache	Set limits to caching of on-demand content, and rename the cache directory.	page 43
Splitting	Modify the protocol to use with pull splitting and whether to allow packet resends.	page 63
Multicasting	Configure back-channel multicasting.	page 87

Security

The security features let you limit connections to Helix Universal Proxy, by client IP address, or by user name and password..

Security Features

Feature	Function	Reference
Access Control	Limit media player connections by IP address.	page 95
User Databases	Select authentication databases.	page 106
Realms	Create authentication realms.	page 108
Authentication	Enable authentication and choose no-authenticate sites.	page 109

Logging and Monitoring

The logging and monitoring features let you view current Helix Universal Proxy activity, as well as review past, recorded activity.

Logging and Monitoring Features

Feature	Function	Reference
Proxy Monitor	Display statuses of current connections.	page 117
Access and Error Logging	Compile user and error statistics.	page 139
Custom Logging	Create templates for reports.	page 143

Restarting Helix Universal Proxy

Some configuration changes you make to Helix Universal Proxy require a restart, which breaks open connections for live events or clips streamed on demand. It's best, therefore, to make these changes during periods of low use. The Helix Administrator interface indicates feature changes that require a Helix Universal Proxy restart. It also prompts you when a change requires a proxy restart when you click **Apply**. Click the **Restart Server** button to restart Helix Universal Proxy.

Queuing Changes for a Later Restart

It is not necessary to restart Helix Universal Proxy immediately after you make a configuration change. In this case, the **Pending Changes** flag appears in the upper-right corner of Helix Administrator. This flag reminds you that all pending changes will go into effect the next time Helix Universal Proxy is started.

Importing Manual Changes on UNIX

If you change the Helix Universal Proxy file manually on a UNIX computer, you can use `SIGHUP` to upload the changes to Helix Universal Proxy without breaking any open connections, as long as the changes do not require a full server restart. To have Helix Universal Proxy re-read the configuration file, use the following `SIGHUP` command:

```
kill -HUP processID
```

in which *processID* is the Helix Universal Proxy process number, as shown in the `Logs/rmproxy.pid` file. For more on this, see "Process ID (PID)" on page 30.

Tip: Helix Administrator indicates when changes require a full restart. Use it as your guide to changes that you can and cannot upload with `SIGHUP`.

For More Information: For more on configuration files, see Appendix A.

License File Information

The text-based license file resides in the `License` subdirectory of Helix Universal Proxy's installation directory. It is in an XML format that you can read with any text editor. Making any changes invalidates the file, however. You can also display the license file through Helix Administrator by clicking **About**. You generally do not need to do anything with the license file, as long as Helix Universal Proxy reads it correctly on startup.

Tip: If you have multiple license files, Helix Administrator shows the values for all of them at once. In this case, you need to read each file individually and calculate additive features, such as the total number of licensed streams.

If all license files are invalid, Helix Universal Proxy will report an error message, add the error to the error log file, and shut down. To resolve this, contact RealNetworks for a valid license file.

Quick Start for Helix Universal Proxy

In this section, you'll use RealOne Player to first play content directly from a Helix Universal Server, and then you'll configure and use RealOne Player to go through Helix Universal Proxy to get the same content.

Before you begin, you'll need the following software on your system:

- Helix Universal Proxy
- RealOne Player (available for free download from **http://www.real.com**).
- A Web browser

You can install the software on different computers, but the computer on which RealOne Player is running needs a sound card and speakers (so that you can see and hear that all the software is working).

The steps for getting started are:

Step 1: Use RealOne Player to Play Content from a Helix Universal Server

Using RealOne Player, test your network connection by playing sample content from a Helix Universal Server. You can use any of the following as sources for the test material:

- any channel listed in RealOne Player's Channel page
- clips streamed from your own Helix Universal Server
- sample content included in the free Helix Universal Server Basic (downloadable from **http://www.realnetworks.com**)

Make a note of which clips you played; you'll use this again later, to test Helix Universal Proxy in " Step 5: Play Content Again".

Step 2: Start Helix Universal Proxy

Common methods for starting Helix Universal Proxy are listed below.

There are also other options for startup, and more details, described in "Starting Helix Universal Proxy" on page 28.

Windows NT Operating System

When you install Helix Universal Proxy on Windows NT or Windows 2000, by default it installs itself as a service, and runs automatically. If it isn't running, from the **Start** menu, select **Programs>Helix Proxy>Helix Proxy**. This starts the `rmproxy.exe` program with the default configuration file, `rmproxy.cfg`.

UNIX-Based Operating Systems

Navigate to the Helix Universal Proxy main installation directory and type the following:

```
Bin/rmproxy rmproxy.cfg
```

Step 3: Monitor Helix Universal Proxy Activity

Start Helix Administrator, and use the Proxy Monitor to see that Helix Universal Proxy isn't in use.

> **Tip:** If you are using Helix Universal Proxy on Windows NT or Windows 2000, you can double-click the Helix Administrator icon on your desktop and skip the steps below.

➤ To start Helix Administrator:

1. Start a Web browser from anywhere on your network.
2. In the browser's address or location box, type the following URL, substituting your values for *address* and *AdminPort*:

   `http://`*address*`:`*AdminPort*`/admin/index.html`

   The setup program generates a random value for `AdminPort` if you did not supply one.
3. You are prompted for your user name and password. Use the same user name and password you created during installation.
4. Click **OK**. Helix Administrator starts.
5. In the left-hand frame, click **Logging & Monitoring**, then click **Proxy Monitor**.

   The monitor page appears in the right-hand frame. Notice that all the numbers in the columns show a value of zero.

Step 4: Configure RealOne Player To Use Your Helix Universal Proxy

Helix Universal Proxy generally doesn't tell clients to contact it; you must explicitly configure clients to use Helix Universal Proxy.

> **Note:** Alternately, you can set up your firewall to intercept requests for streaming media with a device such as a layer-4 switch. In this case, Helix Universal Proxy can intercept client requests without any client configuration.

For this quick start, use the steps below to configure your RealOne Player to use Helix Universal Proxy.

➤ To configure RealOne Player:

1. In RealOne Player, select **Tools>Preferences**.

2. Open the **Connection** category and select **Proxy**.
3. Select the **PNA proxy** checkbox and type the IP address or host name of your Helix Universal Proxy computer in the box next to it.
4. In the **Port** box, type `1090`, the default PNA listening port.
5. Select the **RTSP proxy** checkbox and type the IP address or host name of your Helix Universal Proxy computer in the box next to it.
6. In the **Port** box, type `554`, the default RTSP listening port.
7. Click **OK**.

Step 5: Play Content Again

Now that RealOne Player is configured to always contact Helix Universal Proxy, use RealOne Player to play the same content you used in Step 1.

Step 6: Monitor Helix Universal Proxy Again

Look at the Proxy Monitor in Helix Administrator. The numbers are different, demonstrating that your RealOne Player is now sending its requests to Helix Universal Proxy, rather than directly to the Helix Universal Server.

CHAPTER

4

PROXY SETUP

This chapter describes basic Helix Universal Proxy setup. These functions include specifying ports, binding to IP addresses, and enabling pull splitting amoung others. You may not need to change any of these settings depending on your system's configuration and the values you chose during installation.

Regardless of which features are in use, certain important settings apply to every Helix Universal Proxy. They are described in this chapter.

Basic Proxy Features

At installation, each of the methods Helix Universal Proxy uses to send clips to clients, (pass-through, cache, and pull splitting) are ready to use immediately. There is no need to perform further configuration for basic proxy features to work. This section provides additional information in case you choose to add more functionality.

Pass-through

Pass-through mode is always enabled. It can't be turned on or off.

Cache

The media cache is enabled by default. You do not need to make any changes to begin using the cache automatically.

The cache feature uses the following settings, which are pre-configured:

- **Enable Caching**—the feature is set to `Enabled` by default.

- **Maximum Cache Size**—This is the largest the cache will grow before removing Least Requested URLs (see "Changing the Size of the Cache" below).
- **Cache Directory**—The directory location of the main cache file structure. The default directory is `Cache`.

Changing the Size of the Cache

Once the cache has reached its maximum size, Helix Universal Proxy removes the media which were requested the least often. This method is called Least Recently Used.

> **Tip:** It's a good idea to make the cache size as large as you can, since the more you can cache, the more bandwidth you can conserve.

➤ To change the size of the cache:

1. In Helix Administrator, click **Proxy Setup**. Click **Cache**.
2. In the **Maximum Cache Size** list, type the largest size you want the cache to reach, in megabytes. (The default value is 1000 megabytes. The minimum value you can use is 11 megabytes.)
3. Click **Apply**.

Pull Splitting

When a client requests a live stream, Helix Universal Proxy checks to see if the Helix Universal Server acting as an origin transmitter is configured for pull splitting. Helix Universal Proxy then gets the live stream using the highly efficient pull splitting connection.

Pull splitting is enabled by default.

Helix Universal Proxy uses the following settings to perform pull splitting (you can view them by clicking **Proxy Setup>Splitting** in Helix Administrator), and they are pre-configured:

- **Attempt to Split All Live Broadcasts—** enables/disables Helix Universal Proxy's ability to use pull splitting.
- **Live Splitting Transport—** Defines the transport-layer protocol to use with pull splitting. Initially, Helix Universal Proxy expects to receive origin transmitter streams using the UDP transport. If UDP traffic is prohibited

to the Helix Universal Proxy, it will automatically attempt TCP. Automatic transport negotiation can be disabled by configuring the proxy to always use UDP or TCP.

> **Note:** Note that origin transmitter streams arriving at the Helix Universal Proxy using TCP may result in client rebuffering or greater start-up latency upon client connection.

- **Enable Resends**— In the case of network transmission errors, this setting allows data packets to be resent. By default, this feature is enabled.

Pull splitting with RealSystem Server version 8

If you are using RealSystem Server 8 with Helix Universal Proxy for pull splitting, you'll need to modify the value of a variable in Helix Universal Proxy's configuration file, `rmproxy.cfg`.

> **Warning!** Because editing the configuration file with a text editor can potentially disable Helix Universal Proxy, be sure to read Appendix A before attempting modifications.

➤ To enable pull splitting with RealSystem Server version 8:

1. Make sure Helix Administrator is not in use.
2. Open the configuration file in a text editor. (The default configuration file is `rmproxy.cfg`, located in the main Helix Universal Proxy installation directory.)
3. Find the variable `Splitter_DoubleURLEnable`, and change its value from `0` to `1`. This is how the variable should appear:
   ```
   <Var Splitter_DoubleURLEnable="1"/>
   ```
4. Save and close the configuration file.

Multicasting

Multicasting is enabled by default. Instructions on configuring Helix Universal Proxy to perform multicasting are located in Chapter 8, "Multicasting".

Defining Communications Ports

At installation, you created port settings which tell Helix Universal Proxy where to listen for requests using a particular protocol. You can view the settings from Helix Administrator by clicking **Proxy Setup>Ports**.

- **RTSP Port—** the port where Helix Universal Proxy listens for RTSP requests (these begin with `rtsp://`). At installation, the value is `554`.

  > **Note:** To use a port lower than 1024 on a UNIX system, you must be logged on as super-user.

- **PNA Proxy Port—**the port where Helix Universal Proxy listens for material requested using PNA (these begin with `pnm://`). The default value is `1090`.
- **MMS Port**—the port where Helix Universal Proxy listens for MMS requests (for live or on-demand Windows Media clips). The default value is `1755`.
- **Admin Port**—port number to which Helix Administrator connection requests are directed. The value for this setting is selected at random during setup to ensure security, and can be overridden by the user during setup.

If you change the port numbers for RTSP Port and PNA Port after setting up clients for the first time you will need to reconfigure RealNetworks media players to include the new ports. (If Helix Universal Proxy is no longer listening on ports designated in the client, it will not receive the request.)

The same is true if you change the port number for MMS Port. You'll need to reconfigure Windows Media Player to include the new port number.

> **Note:** If your Helix Universal Proxy and another application that uses ports are on the same machine, you may need to modify the HTTP Port setting. See "Running Other Applications and Helix Universal Proxy on the Same System" on page 50 for additional information.

In addition to the actual port settings, there are other global settings that deal with how ports operate on Helix Universal Proxy. Descriptions for these features are as follows:

- **Create user names and passwords for Administrators**—clicking on the word "Create" takes you to **Security>Realms**, where you can create new administrator user names and passwords for Helix Universal Proxy. For more information, see "Authenticating Helix Administrator Users".

- **UDP Resend Port Range**—blank by default. Forces Helix Universal Proxy to use a minimum number of UDP ports to service UDP replies from client software. Enter a minimum range of two ports for each CPU. For more information, see "Modifying Shared UDP Port Ranges".

Binding To An IP Address

When Helix Universal Proxy starts, it uses the IP address assigned to the first network interface it finds on the computer—network interface 0. In a computer with multiple network interfaces—often referred to as a *multi-homed* machine—you can configure Helix Universal Proxy always to use specific IP addresses. Through this feature, you can select individual IP addresses to use, or you can bind to all the IP addresses on the machine.

Using Localhost

By default, Helix Universal Proxy binds to the *localhost* address (also called the *loopback* address), which enables a simulated network connection from Helix Universal Proxy to a client installed on the same computer. When using this address, which is useful for testing, no information is sent over the network, but it appears as if the connection came from the network. You can express this address in dotted decimal form as `127.0.0.1`.

Capturing All Addresses

You can use the IP binding feature to capture all addresses for Helix Universal Proxy's use. To do this, specify the IP address `0.0.0.0`, and delete all others. Helix Universal Proxy will automatically bind to all addresses and to localhost. For most installations, RealNetworks recommends binding to all addresses.

Binding to Specific Addresses

If you bind Helix Universal Proxy to one or more specific addresses, Helix Universal Proxy binds only to those addresses, but not to others. In other words, it will not bind to localhost. To bind to a specific address and to localhost, you must add both to the IP binding list.

> **Note:** If a firewall is in use, you may need to configure it to allow traffic to pass on the addresses you added to the IP

Binding list. See "Working with Multiple IP Addresses" for information.

Modifying IP Addresses

You bind Helix Universal Proxy to IP addresses using Helix Administrator. You'll need to restart Helix Universal Proxy after making these changes.

➤ To reserve IP addresses for Helix Universal Proxy:

1. In Helix Administrator, click **Proxy Setup> IP Binding**.
2. Click the "+" icon and type the IP address that you want Helix Universal Proxy to use into the **Edit IP Address** box.

   Warning! Type the address carefully. If you type an IP address that does not exist on this computer, Helix Universal Proxy will not be able to restart or to start.

3. Repeat this procedure for each address on this machine that you want Helix Universal Server to use.

   Warning! Use either `0.0.0.0` or specific addresses, but never both. If you use both, Helix Universal Proxy will not start.

4. Click **Apply**.

Managing Bandwidth

You can manage the bandwidth consumption on your network by limiting the connections made by Helix Universal Proxy, and the total bandwidth allowed between the proxy and the server, and the proxy and the client. For more information, see Chapter 9, "Bandwidth Management".

Proxy Routing

You can route streaming media traffic from one Helix Universal Proxy to various other parent proxies based on the URL received from the RealOne Player. For more information, see "Proxy Routing" on page 75.

Redundant Proxies

You can set up your network so it continues to route streaming media traffic through a separate, parallel Helix Universal Proxy when the network connection to your primary Helix Universal Proxy goes down. For more information, see "Working With Redundant Proxies" on page 80.

Administering Both Helix Universal Proxy and Helix Universal Server

If you are the administrator of both Helix Universal Proxy and Helix Universal Server (for example, if you administer a corporate Web presence for both internal (Helix Universal Proxy) and external (Helix Universal Server) use, or if you are an ISP host and you offer Helix Universal Server streaming services to your clients), here are some things to keep in mind:

- **Configuration file**—the structure of the configuration file is the same; however, certain sections are unique to Helix Universal Proxy.
- **Access log**—Helix Universal Proxy's access log uses a similar structure as Helix Universal Server, with additional information about the proxy appended to the end of each record.
- **Pull splitting—**Helix Universal Proxy's pull splitting method is nearly identical to the Helix Universal Server method of pull splitting, but Helix Universal Proxy does not need to include the transmitting Helix Universal Server in the URL.
- **Multicast**—Helix Universal Proxy has only one method of multicast, which is the same as Helix Universal Server's back-channel multicast. However, Helix Universal Proxy can only multicast those incoming streams which are enabled for pull splitting on the Helix Universal Server acting as the origin transmitter.
- **Authentication—**Like Helix Universal Server, Helix Universal Proxy authenticates users who access Helix Administrator. Unlike Helix Universal Server, however, Helix Universal Proxy does not perform authentication on a per-clip basis. Instead, it allows or denies player access to specific Helix Universal Servers by looking at the host name or address of the origin Helix Universal Server.

Running Other Applications and Helix Universal Proxy on the Same System

If you install Helix Universal Proxy on the same system as other applications that use ports to exchange data, you may need to complete additional steps to ensure that the other application (a Web server for example) and Helix Universal Proxy are not attempting to use the same ports. For example, most Web servers use port 80 for HTTP requests. During installation, Helix Universal Proxy can set the default HTTP port value to 8080, but if you decide to configure Helix Universal Proxy to use port 80 (the same port as the Web server), problems may ensue. You may have to perform the following steps:

- Choose a different port for Helix Universal Proxy to use for HTTP.
- Reserve an IP address for Helix Universal Proxy.

Change the HTTP Port Value

Helix Universal Proxy does not use the HTTP port to deliver media, however the shared code between Helix Universal Proxy and Helix Universal Server requires that an HTTP port setting be defined during the installation of Helix Universal Proxy. RealNetworks recommends accepting port 8080 to avoid conflicts.

If you do have to change the HTTP port setting after installation, you'll need to edit the configuration file, `rmproxy.cfg` (or one with another name) manually.

> **Warning!** Because editing the configuration file with a text editor can potentially disable Helix Universal Proxy, be sure to read Appendix A before attempting modifications.

➤ To modify the value of HTTP Port after installation of Helix Universal Proxy:

1. Make sure Helix Administrator is not in use.
2. Open the configuration file in a text editor. (The default configuration file is `rmproxy.cfg`, located in the main Helix Universal Proxy installation directory.)
3. Find the variable `HTTPPort`, and change its value to `8080`, or another value that won't conflict with other applications.
4. Save and close `rmproxy.cfg`.

Set IP Binding List

You may need to reserve at least one IP address for Helix Universal Proxy's use, and instruct your Web server not to use that address. This requires a multihomed machine. See "Binding To An IP Address".

Setting UNIX Features

Setting User and Group Names

By default, Helix Universal Proxy on UNIX uses the user and group names of the person who starts it. After startup, though, it can immediately switch to a different user and group setting. This lets you start Helix Universal Proxy as `root`, so that it can capture port 554 for RTSP communications, then assume a different user and group identity. The user and group names must be predefined through the operating system, and must have write permission for Helix Universal Proxy's `Logs` and `Cache` directories, also the Helix Universal Proxy configuration file.

➤ To change the group or user names:

1. In Helix Administrator, click **Proxy Setup>User/Group Name**.
2. Type the user name or ID number in the **User Name or ID** box. The default is `%-1`, which means Helix Universal Proxy uses the name of the user who logged in and started Helix Universal Proxy.
3. Type the user name or ID number in the **Group Name or ID** box. The default is `%-1`, which means that Helix Universal Proxy uses the group name of the user who logged in and started Helix Universal Proxy.
4. Click **Apply**.

Setting Processor Count

On systems with multiple CPU processors, the `ProcessorCount` variable should be set to the number of processors available to Helix Universal Proxy. If this variable is not present, Helix Universal Proxy will use its automatic processor test, but the test may not be accurate if the system is busy doing other things when the test is performed. In addition, if you are running Helix Universal Proxy with a user ID other than root, the CPU detection system is not enabled.

The default value of `0` for the `ProcessorCount` variable means that Helix Universal Proxy will use its test to determine the number of processors available. If you have more than one processor on your system, you should manually configure the processor count by editing the configuration file (be sure to make a backup copy of the configuration file before you begin editing).

1. Open your `rmproxy.cfg` file and edit the `<Var ProcessorCount="0"/>` variable to the proper number of processors on your machine. For example, on a host system with two processors, the setting is:

   ```
   <Var ProcessorCount="2"/>
   ```

2. Save the changes made to your configuration file.

3. Start the `rmproxy` process with the `--sct` command. For example:

   ```
   ./rmproxy ../rmproxy.cfg -m 512 --sct &
   ```

   starts Helix Universal Proxy with 512 MB of memory while skipping the CPU detection test.

CHAPTER

5

CLIENT CONFIGURATION

For client software (such as RealOne Player) to contact and use your Helix Universal Proxy, you either explicitly configure the clients to connect to Helix Universal Proxy, or use an L4 switch or router to automatically direct client requests to Helix Universal Proxy. This chapter describes how to set up RealOne Player and Windows Media Player to contact Helix Universal Proxy.

Overview

Most clients, such as RealOne Player, contain an option to contact a proxy rather than sending requests directly to Helix Universal Servers. In the client software, the user types the IP address (or host name) and port number of the proxy software to contact.

If you choose to connect clients to your Helix Universal Proxy this way, you must either set up your users' client software yourself or send instructions to the users on how to set up the software themselves.

Configuring RealOne Players to Contact Helix Universal Proxy

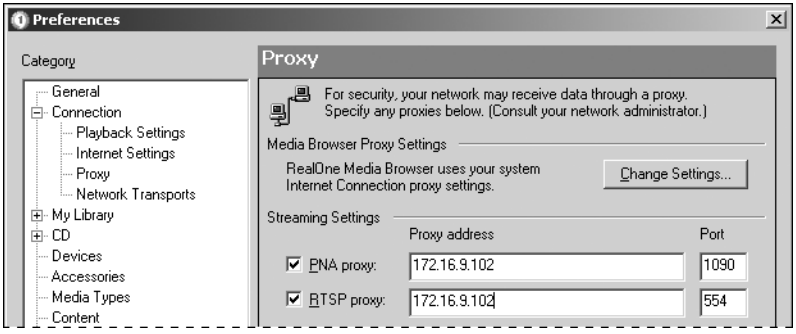
If you choose to configure RealOne Players to connect directly to Helix Universal Proxy, use the instructions in this section.

➤ To configure RealOne Player:

1. In RealOne Player, select **Tools>Preferences**.
2. Open the **Connection** category and select **Proxy**.
3. Select the **PNA proxy** checkbox.
4. In the box next to it, type the IP address or host name of your Helix Universal Proxy computer.

5. In the **Port** box, type the number of the Helix Universal Proxy port number to which this client should send its PNA requests (usually `1090`). The number you type here must match the number in the **PNA Proxy Port** box on the Ports page in Helix Administrator.
6. Select the **RTSP proxy** checkbox.
7. In the box next to it, type the IP address or host name of your Helix Universal Proxy computer.
8. In the **Port** box, type the number of the Helix Universal Proxy port number to which this client should send its RTSP requests (usually `554`). The number you type here must match the number in the **RTSP Port** box on the Ports page in Helix Administrator.
9. Click **OK**.

RealOne Player Proxy Preferences Page



Configuring Windows Media Players to Contact Helix Universal Proxy

If you choose to configure Windows Media Players (version 7.1 or later) to connect directly to Helix Universal Proxy, use the instructions in this section.

➤ To configure Windows Media Player:

1. In Windows Media Player, select **Tools>Options**.
2. Select the **Network** tab.
3. Under Proxy Settings, select **MMS**.
4. Click the **Configure...** button.

5. Select the **Use the following proxy server** radio button.
6. In the **Address:** text box, type the IP address or host name of your Helix Universal Proxy computer.
7. In the **Port** box, type the number of the Helix Universal Proxy port number to which this client should send its MMS requests (usually 1755). The number you type here must match the number in the **MMS Port** box on the Ports page in Helix Administrator.
8. Click **OK**.

CHAPTER

6

FIREWALLS

Firewalls may present communications problems to Helix Universal Proxy. This chapter helps you to become familiar with network firewalls to help you use Helix Universal Proxy successfully. It first provides background on firewalls and network protocols. It then recommends ways to work with firewalls to give viewers the best possible streaming media experience. Finally, it lists the communications ports that RealNetworks components use.

How Firewalls Work

A firewall is a software program or device that monitors, and sometimes controls, all transmissions between an organization's internal network and the Internet. However large the network, a firewall is typically deployed on the network's edge to prevent inappropriate access to data behind the firewall. The firewall ensures that all communication in both directions conforms to an organization's security policy.

Firewall technologies are configurable. You can limit communication by direction, IP address, protocol, ports, or numerous other combinations. Firewalls positioned between your Helix Universal Proxy and other computers may cause communication failures if the firewall does not allow for the types of communication Helix Universal Proxy requires. These other computers may be media clients or servers set up as origin transmitters.

If you have access to the firewall, you can configure it to enable the ports, protocols, and addresses that optimize Helix Universal Proxy communication. In some cases, however, your organization's security policy may prevent optimal streaming. For example, firewalls configured to only allow TCP traffic may cause the user to see frequent buffering of clips. User experience of the presentation is compromised; greater latency and startup times affect the time needed to view the clip, and delivery of the clip requires more total bandwidth.

Protocol Layers

A protocol is a language that computers use when communicating over a network. The Transmission Control Protocol/Internet Protocol—commonly called TCP/IP—encompasses a suite of protocols upon which the Internet is built. TCP/IP protocols work on a layering principal, in which each layer is assigned a specific network task.

For communication to occur, a source computer sends a message from its highest network layer to its lowest. The lowest network layer at the source forwards the message over the network. When the message arrives at the destination computer, it must pass through the exact same layers, but in reverse order.

Each network layer uses specific protocols to perform its task. Packets passed down from upper layers are tucked inside lower layer packets. This is called *encapsulation*. By encapsulating packets, a layer can handle its responsibilities without understanding the preceding layer. Through this layering scheme, a destination layer on one computer receives exactly the same object sent by the corresponding source layer on another computer.

For example, an application such as a Web browser packages data, such as a Web page request made over HTTP, at the application layer, passing it to the lower transport layer. There, the HTTP request packets are bundled into TCP packets that are then delivered to destination Web server. When the Web server receives the source TCP packets, it strips off the TCP shells, and bumps the HTTP message up to the destination computer's application layer. This layer, in turn, delivers to the HTTP-based request to the Web server.

> **Note:** Network layering is a complex topic. This section omits discussion of additional layers required to deliver packets over a network, focusing instead on the transport and application layers, and the protocols relevant to streaming media for each.

Transport-Layer Protocols

All transport-layer protocols transfer data between hosts. The transport-layer protocol in use can greatly affect the quality of the stream received. There are two main transport protocols used on IP networks: TCP and UDP. Helix Universal Proxy utilizes both of these protocols, and the choice of protocol is generally negotiated automatically by the Helix Universal Servers and clients involved.

Transmission Control Protocol (TCP)

Helix Universal Proxy can use TCP in a number of ways. Because TCP offers a single channel for bi-directional communication, Helix Universal Proxy uses it as a control channel to relay commands from clients to Helix Universal Server about passwords and user commands such as pause and fast-forward. The TCP protocol also guarantees delivery of packets, and has built-in congestion control that helps to provide reliable communication.

On the down side, TCP responds slowly to changing network conditions, and creates network overhead through its error checking facility. For this reason, TCP is best suited for delivering low-bandwidth material like passwords or user commands. In some cases, TCP can facilitate communication through a firewall. For example, firewalls that block UDP traffic between Helix Universal Proxy and its clients may permit TCP connections.

User Datagram Protocol (UDP)

Helix Universal Proxy uses UDP packets to deliver data to client software on its data channel. Client software sends UDP-based requests to Helix Universal Proxy (which get relayed to Helix Universal Server) when packets on the data channel have not arrived. Because the transport does not consume as much network overhead, it can deliver packets faster than TCP.

Because video and audio data typically consume large amounts of bandwidth, it makes the most sense to use UDP to deliver streaming media. For this reason, origin Helix Universal Servers use UDP as the default for server-to-proxy communication.

Application-Layer Protocols

Helix Universal Proxy uses three application-layer protocols to deliver streaming media to clients: RTSP, PNA, MMS. The following table summarizes their use.

Application-Layer and Transport-Layer Protocols

Player Software	Application Protocol	Transport Options
RealOne Player, RealPlayer, QuickTime Player	RTSP	TCP and UDP, or TCP only
Windows Media Player	MMS	TCP and UDP, or TCP only
RealPlayer 5 and earlier	PNA	TCP and UDP, or TCP only

Real-Time Streaming Protocol (RTSP)

A standards-based protocol designed for serving multimedia presentations, RTSP is very useful for large-scale broadcasting. Only RTSP can deliver SureStream files with multiple bit-rate encoding. SMIL, RealText, and RealPix also require RTSP. RTSP uses TCP for player control messages, and UDP for video and audio data. RTSP can also use TCP to deliver data, but this is not recommended. Use RTSP with RTSP-compatible players such as RealOne Player, RealPlayer, and QuickTime Player.

Progressive Networks Audio (PNA)

PNA is a proprietary protocol used in earlier RealNetworks client software versions. PNA is supported in the current Helix Universal Proxy for compatibility with older RealNetworks clients (RealPlayer 5 and earlier). PNA uses TCP for player control messages, and UDP for audio data. PNA can also use TCP to deliver data, but this is not recommended.

> **Note:** The PNA protocol uses `pnm://` rather than `pna://` in the request URL.

Microsoft Media Services (MMS)

The MMS protocol is designed specifically for serving multimedia presentations. Although it is not standards-based, you can use it to broadcast live or on-demand Windows Media clips to Windows Media Player. MMS uses TCP for player control messages, and UDP for video and audio data. MMS can also use TCP to deliver data.

HyperText Transfer Protocol (HTTP)

HTTP is typically used for Web pages. With Helix Universal Proxy, HTTP is used to display Helix Administrator pages and HTML-based documentation.

Packet Formats

All Internet data is delivered in IP packets. But just as TCP or UDP can encapsulate a control protcol for streaming media, IP packets can encapsulate data packets in formats designed to deliver streaming media data. Helix Universal Proxy uses the RDT and RTP packet formats—either of which can be delivered in either TCP or UDP internet protocol.

RealNetworks Data Transport (RDT)

When Helix Universal Proxy communicates to a RealNetworks client such as RealOne Player over RTSP, it uses RDT as the packet format. A proprietary format, RDT allows the use of RealMedia features such as SureStream.

Real-Time Transport Protocol (RTP)

RTP is a standards-based packet format designed as the companion to the RTSP protocol. QuickTime Player, for example, uses RTP as its packet format. Helix Universal Proxy fully supports RTP, and shifts to RTP automatically when streaming to an RTP-based client such as QuickTime Player. RealNetworks clients such as RealOne Player also support RTP, using this format when receiving data from RTSP/RTP servers.

Communicating with Software Behind Firewalls

Information in this section applies to administrators of Helix Universal Proxy who are interested in the nature of the connection between Helix Universal Proxy and other RealNetworks software.

Communicating with Clients Behind Firewalls

Helix Universal Proxy uses two connections, known as *channels*, to communicate with clients:

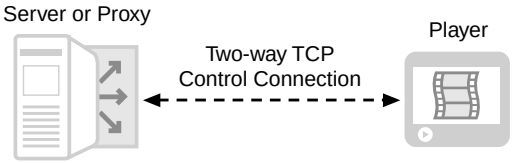
- control channel

  Helix Universal Proxy uses this channel for communication with the client. Over this channel, Helix Universal Proxy initially requests and receives passwords, sends information to the client about the requested media such as the name, length, and copyright of the clip. Clients send instructions such as fast-forward, pause, and stop.

- data channel

  Once the control channel is established, media clips themselves are streamed over a separate *data channel*.

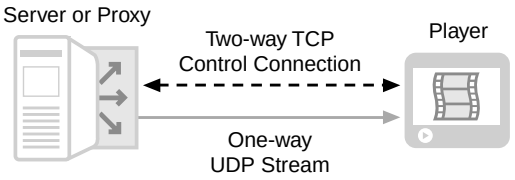
Initial Connection Between Helix Universal Server and Client, or Between Helix Universal Proxy and Client



At the transport layer, most media players, including RealOne Player, can work around situations in which the first communication fails because the player resides behind a firewall that blocks the preferred protocol. The primary strategy involves shifting automatically to protocols and delivery methods that aren't blocked. Typically, the client shifts the control channel to the less efficient TCP, which is less likely to be blocked than UDP.

If the control connection is established, the client then negotiates the data channel.

Data Channel Between Helix Universal Server and Client, or Between Helix Universal Proxy and Client



Optimally, the data channel will use the more efficient UDP transport. If the stream is live, some client software, including RealOne Player, attempts to set up a UDP multicast first. If this method fails, the client next attempts UDP unicast. And if that fails, the client uses the established control channel for data. In short, the client tries to set up the most optimal data delivery method, relying on the control connection as a last resort.

> **Note:** At the application-layer, Helix Universal Proxy connects with RTSP using UDP or if necessary, TCP for data connections. Helix Universal Proxy has no option for HTTP delivery. Thus, if the firewall prohibits RTSP, Helix Universal Proxy will not be able to proxy streams on behalf of clients.

Specific Protocols and Port Settings

The list below shows how the client software determines what protocol it will ask Helix Universal Proxy to use in sending the streamed media over the data channel.

1. The client attempts to open a control connection, using TCP. It uses port 554 for the RTSP protocol, or port 7070 for the PNA protocol.
   - If the firewall does not allow TCP on 554 (or port 7070), the request is denied and the user sees an error message.
   - If the firewall permits the TCP connection, the client goes to Step 2.
2. Now that a TCP control connection has been established, the client attempts to set up the data channel.

   If the request is for on-demand content, the client tries these methods:

   a. First, it tries UDP, in the range of port 6970 through 32000. (Earlier versions of RealPlayer used a smaller range. Consult the "RealPlayer versions 3 through 5 Communication Ports" table.)

   b. If UDP is not allowed, it requests that the data be sent using TCP on the established control channel.

   If the request is for live content, the client tries three connection methods:

   a. First, it tries to use multicast. This is a specialized option not available on many networks. Multicast uses the UDP transport protocol and may use either the RTSP or PNA application-level protocol. Firewalls must be specially configured to allow multicast traffic.

   b. If multicast is not available, the client requests that the material be sent using UDP on ports 6970 through 32000.

   c. If UDP cannot pass through the firewall, the client requests delivery using TCP on the established control channel.

Users can configure clients to always use a particular protocol and port as directed by their firewall administrator. For more information, refer to the online help of your client software for instructions on setting preferences.

Allowing Pull Splitting to Work Through Firewalls

By default, Helix Universal Proxy and Helix Universal Server are set to auto-negotiate the splitting transport, favoring UDP over TCP. Optionally, both products can use TCP exclusively.

➤ To change the protocol for Server-to-Proxy split communication:

1. In Helix Administrator, click **Proxy Setup**. Click **Splitting**.
2. In the **Live Splitting Transport** box, select **Always Use TCP**.
3. Click **Apply**.

Working with Multiple IP Addresses

If your firewall expects to allow connections to Helix Universal Servers only from certain IP addresses, make sure that it permits traffic on all the addresses used in the IP Bindings list.

When the machine on which Helix Universal Proxy is running has multiple IP addresses (either multiple Network Interface Cards or virtual addresses), and you use the IP Bindings feature to instruct Helix Universal Proxy to use those addresses, Helix Universal Proxy will make its outgoing connections using the operating system's routing table. Refer to your operating system's TCP/IP documentation for more information.

Firewall Configurations (For Firewall Administrators)

This section describes firewall types, the best way to configure your firewall to permit streaming media, and lists the port numbers used by Helix Universal Proxy.

Firewall Types

Firewalls can be categorized into roughly six types. A particular firewall vendor may combine more than one type into a particular product. The type of firewall in use by your organization will affect the method that Helix Universal Proxy uses to stream content to clients.

- Application-level proxy
- Transparent proxy
- Packet filter
- Stateful packet filtering
- SOCKS
- Network address translation

The address that appears in the access log of the origin Helix Universal Server or Helix Universal Proxy depends on the client's type of firewall.

A firewall monitors every type of transmission between client software and the Internet, however, this discussion looks only at the firewalls' effects on streaming media.

Application-Level Proxy Firewall

Application-level firewalls first determine if a requested connection between a computer on the internal network and one on the outside is permitted. If the connection is authorized, the firewall mimics the requesting software and sets up the necessary communication links between the two computers. As an intermediary, the firewall can monitor the communication between the two networks and suppress any unauthorized activity.

Because an application-level firewall acts as an intermediary between RealOne Player and Helix Universal Proxy (or between Helix Universal Proxy and Helix Universal Server), the firewall itself must know how to handle the RealOne Player protocols (RTSP and PNA).

The user must configure the client software to contact a proxy or firewall machine. (In RealOne Player, this setting is located under **Tools>Preferences>Connection>Proxy**.)

Transparent Proxy Firewall

A network administrator configures the firewall to intercept requests for streaming media.

Packet Filter Firewall

Rather than impersonating an application, network-level firewalls examine the packets of information sent at the transport level to determine whether a particular packet should be blocked. Each packet is either forwarded or blocked based on a set of rules defined by the firewall administrator.

A common configuration for network-level-filtering firewalls is to allow all connections initiated by machines inside the firewall, and to restrict or prohibit all connections made by machines outside the firewall. For most programs, this works well since they usually only establish a single outbound TCP connection.

However, RealOne Player and Helix Universal Proxy (or Helix Universal Proxy and Helix Universal Server) maintain two simultaneous connections: a TCP

connection for sending commands and a UDP connection to stream the actual media according to the instructions received from TCP. The TCP connection initiated by the player for controlling the connection will work through a packet filter firewall. Since network-level filters block UDP as a matter of course, the UDP stream sent by the Helix Universal Server or by Helix Universal Proxy will be deflected off the firewall and never reach the player that made the request.

Stateful Packet Filtering Firewall

A stateful packet filtering firewall monitors the communication between the client and the Internet to ensure that inbound packets are being sent at the request of a client inside the firewall. Similar to packet filters, it may include additional options that allow more sophisticated actions to be taken with individual packets.

These firewalls should be configured to permit RTSP and PNA traffic.

Network Address Translation Firewall

A network address translation firewall converts the client's internal address to an external address before it forwards the client's requests to Helix Universal Server. Once it receives a request, Helix Universal Server will send its UDP packets directly to the firewall, rather than to the client, and the firewall may not know which client requested the packets. Network address translation is often implemented as part of packet filtering firewalls or stateful packet filtering firewalls.

SOCKS Firewall

Only software with built-in SOCKS support, that must additionally be configured by the user, can send data through a SOCKS firewall; RealOne Player does not include SOCKS support.

In some cases, a user can install a Winsock.dll that supports SOCKS, and configure it to point to the SOCKS firewall.

Summary of Firewall Types

The table below summarizes the six most common firewall types and any special configuration information.

Streaming Media Over the Firewall Types

	Client configuration required?	IP address seen by the client	IP address seen by the Server (in access log)	Valid inside addresses required?	RTSP support required to get UDP?	RTSP support required to get TCP?
Application-level proxy	Yes	Firewall's address	Firewall's address	No *	Yes	Yes
Transparent proxy	No	Server	Firewall	No*	Yes	No**
Packet filter	No	Server	Client	Yes	No	No
Stateful packet filtering	No	Server	Client	Yes	No	No
Address translation	No	Server	Firewall	No*	Yes	No
SOCKS	Yes	Firewall	Firewall	No*	No***	No

* Usually requires compliance with RFC 1597 Address Allocation for Private Internets (http://www.ietf.org/rfc/rfc1597.txt)
** May require special configuration
***Requires SOCKS version 5.0

Some firewalls are actually a mix of the firewall types described in the preceding section.

Depending on the type of firewall and its location, the client address shown in the access log may not reflect the true address of the client. The table below

lists the address that will appear in the access log as the requesting client's address.

Address Shown in Access Log

Firewall type	Firewall between client and Helix Universal Proxy	Firewall between Helix Universal Proxy and Helix Universal Server	
	Address shown in Helix Universal Proxy's access log	Address shown in Helix Universal Proxy's access log	Address shown in Helix Universal Server's access log
Application-level proxy	Firewall's address	Client	Firewall's address
Transparent proxy	Firewall	Client	Firewall
Packet filter	Client	Client	Helix Universal Proxy
Stateful packet filtering	Client	Client	Helix Universal Proxy
SOCKS	Firewall	Client	Firewall
Address translation	Firewall	Client	Firewall

Best Firewall Arrangements

The firewall that provides the best experience for RealNetworks software users is one that allows streaming media, by enabling TCP and UDP traffic. Refer to the section "Ports Used by RealNetworks Products" on page 70 for a complete list of ports that need to be open.

- Several firewall vendors already include this type of streaming media support. View the RealNetworks firewall page at **http://service.real.com/firewall** to find a vendor.
- You can modify your existing firewall with the help of the free RealNetworks Firewall Administrator's Proxy kit.

The next best option is a firewall that allows a TCP control channel and a TCP data channel. Your firewall administrator can easily make this change to the firewall. However, the quality of the connections will not be as good with this configuration.

Locating Helix Universal Proxy Near the Firewall

A realistic deployment of Helix Universal Proxy within or near a secure network is to place it inside a network firewall or in a secure perimeter

network known as the DMZ, (for de-militarized zone.) In such a deployment, it is typical that clients are not allowed to access the public internet or other non-local networks directly; instead, clients send their requests to Helix Universal Proxy, which is enabled to make and receive Internet connections outside the secure network. In this arrangement, only Helix Universal Proxy is exposed to network traffic beyond the confines of the secure firewall.

The firewall must allow the following types of connections:

- All RealOne Players residing within the secure network need to connect to Helix Universal Proxy using TCP.
- Helix Universal Proxy needs to be able to send both TCP and UDP traffic to its clients.
- If Helix Universal Proxy is contacting Helix Universal Servers acting as origin transmitter that are outside the secure network, the firewall must allow it to make outbound TCP connections on several ports. Additionally, UDP traffic will need to be received by the Helix Universal Proxy from those remote Helix Universal Servers.

Refer to the next section, "Ports Used by RealNetworks Products", for specific information on the ports that are needed.

Ports Used by RealNetworks Products

The following section will help you to decide which ports to open on your firewall. If you do not want to open all the ports listed, refer to the detailed information at **http://service.real.com/firewall**.

These tables do not cover use of port numbers in multicasting.

Helix Universal Proxy Default Ports

The following tables list the default ports used by Helix Universal Proxy.

Communicating with Media Players, Communicating with a Child Helix Universal Proxy

Activity	Port Number	Protocol	Purpose
Listen on	554	TCP	RTSP proxy requests
Listen on	1090	TCP	PNA proxy requests
Listen on	1755	TCP	MMS proxy requests
Send to	6970-65535	UDP	Data channel (port numbers are not configurable)
Send to	1024-5000	UDP	MMS media packet delivery

Communicating with Media Servers

Activity	Port Number	Protocol	Purpose
Send to	554	TCP	Control channel for RTSP, and splitting cache data requests from Helix™ Universal Server version 9.0 & later.
Send to, Listen on	3030	TCP or UDP	Data and control channel for pull splitting using TCP. Control channel for pull splitting using UDP. (Used with RealSystem Proxy and RealSystem Server version 8.02 and earlier.)
Send to	1755	TCP	Control channel for MMS.
Listen on	6970 - 32000	UDP	Data channel for inbound UDP.

(Table Page 1 of 2)

Communicating with Media Servers (continued)

Activity	Port Number	Protocol	Purpose
Send to	7070	TCP	Control channel for PNA requests to Helix Universal Server
Send to	7878	TCP	Cache requests to Helix Universal Server (Used with RealSystem Proxy and RealSystem Server version 8.02 and earlier.)

(Table Page 2 of 2)

Communicating with Helix Administrator

Activity	Port Number	Protocol	Purpose
Send to	9090	TCP	Server Monitor traffic
Listen on	Admin Port	TCP	Helix Administrator

Communicating with a Parent Helix Universal Proxy

Activity	Port Number	Protocol	Purpose
Send to	554	TCP	Control channel for RTSP requests to parent Helix Universal Proxy
Send to	554	TCP or UDP	Data and control channel for pull splitting
Send to	1090	TCP	Control channel for PNA requests to Helix Universal Proxy
Send to	7878	TCP	Cache requests to Helix Universal Proxy (Used with RealSystem Proxy and RealSystem Server version 8.02 and earlier.)
Listen on	6970-32000	UDP	Data channel

Media Player Default Ports

The following table lists the communications ports used by RealOne Player, RealPlayer 6-8, Windows Media Player, and QuickTime Player. In addition to the settings listed below, RealOne Player inherits proxy settings (if they exist) from the default browser, although users can turn off this feature from the RealOne Player **Preferences** menu.

When Helix Universal Proxy receives a control channel request, it directs the data to the port number specified by the client. RealOne Player and RealPlayer choose UDP for the data channel, and indicate a data channel port number between 6970 and 32000. Windows Media Player also chooses UDP, and indicates a data channel port number between 1024-5000. If the client chooses TCP for the data channel, Helix Universal Proxy uses the same port number for both the control channel and the data channel.

Communicating with a Parent Helix Universal Proxy

Activity	Port Number	Protocol	Purpose
Send to	554	TCP	Control channel for RTSP requests to parent Helix Universal Proxy
Send to	554	TCP or UDP	Data and control channel for pull splitting
Send to	1090	TCP	Control channel for PNA requests to Helix Universal Proxy
Send to	7878	TCP	Cache requests to Helix Universal Proxy (Used with RealSystem Proxy and RealSystem Server version 8.02 and earlier.)
Listen on	6970-32000	UDP	Data channel

Media Player Ports for Communication with Helix Universal Server or Helix Universal Proxy

Activity	Port Number	Protocol	Purpose
Send to	7070	TCP	Control channel for PNA requests (data channel also, if TCP was requested)
Send to	554	TCP	Control channel for RTSP requests (data channel also, if TCP was requested)
Send to	1755	TCP or UDP	TCP control channel for MMS requests (data channel also, if TCP was requested); UDP resend requests by MMS
Send to, Listen on	6970-32000	UDP	Data channel

Versions of RealPlayer earlier than RealPlayer G2, use the following ports.

RealPlayer versions 3 through 5 Communication Ports

Activity	Port Number	Protocol	Purpose
Listen on	6970 - 6999	UDP	Data channel (not configurable)

Helix Universal Server Default Ports

The following tables list the default ports that Helix Universal Server uses to communicate with media clients and other servers.

Helix Universal Server Ports for Communicating with Media Players

Activity	Port Number	Transport	Purpose
Listen on	554	TCP	Control channel for RTSP requests (data channel also, if TCP was requested)
Listen on	7070	TCP	Control channel for PNA requests (data channel also, if TCP was requested)
Listen on	8080	TCP	HTTP requests
Send to, Listen on	6970-6999	UDP	Data channel (port numbers are not configurable)

Helix Universal Server Ports for Communication with Helix Universal Proxy

Activity	Port Number	Transport	Purpose
Listen on	3030	TCP or UDP	Data channel for pull splitting requests (Used with RealSystem Proxy and RealSystem Server version 8.02 and earlier.)
Send to	6970-32000	UDP	Data channel (port numbers are not configurable)
Listen on	7802	TCP	Helix Universal Proxy requests (Used with RealSystem Proxy and RealSystem Server version 8.02 and earlier.)
Listen on	7878	TCP	Helix Universal Proxy requests (Used with RealSystem Proxy and RealSystem Server version 8.02 and earlier.)

Modifying Shared UDP Port Ranges

Helix Universal Proxy and Helix Universal Server establish a UDP channel for client packet acknowledgements and packet resend requests. Certain network and firewall configurations might prevent UDP data from being sent between a client and Helix Universal Proxy, or between Helix Universal Proxy and Helix Universal Server. While network prohibitions of this UDP traffic do not halt RTSP communications and client playback, it does restrict the ability of the proxy and server to respond to packet loss, and might contribute to delivery quality degradation. Thus, Helix Universal Proxy and Helix Universal Server now allow all UDP client-originated traffic to be multiplexed through a limited, shared UDP port range, if this configuration is required by your firewall.

➤ To limit the number of ports used for UDP replies:

1. In Helix Administrator, click **Proxy Setup**. Click **Ports**.
2. In the **UDP Resend Port Range** box, enter a minimum range of two ports for each CPU. This feature is blank by default.

   Note: The first port value used in this variable must always be an even number.

CHAPTER

7

PROXY ROUTING AND REDUNDANT PROXIES

Helix Universal Proxy can use other Helix Universal Proxys to route media requests between the Helix Universal Server and RealOne Players. For networks that handle Internet-bound requests with strict rules, you can configure Helix Universal Proxy to route requests for material originating from certain Helix Universal Servers through other Helix Universal Proxys. In addition, you can configure your network to deliver media consistently using more than one Helix Universal Proxy in case one network path should become disabled. This chapter explains how to set up proxy routing, and how to configure redundant proxies.

Proxy Routing

Proxy routing, sometimes known as chaining or parent/child, allows you to route Helix Universal Proxy requests through other Helix Universal Proxys.

The proxy routing feature instructs Helix Universal Proxy to look at the address of the requested material, and to send it either to a specific Helix Universal Proxy, or to send it directly to the Helix Universal Server that hosts the content.

The main Helix Universal Proxy which handles requests bound for the Internet is called the parent Helix Universal Proxy; the Helix Universal Proxys located closest to the clients are called child Helix Universal Proxys.

Typical uses for this feature include routing all requests for locally-served material directly to the Helix Universal Server, and forwarding all other requests through a gateway Helix Universal Proxy.

Notes on Deploying This Feature

A parent Helix Universal Proxy can also stream content to clients while simultaneously streaming data to a child Helix Universal Proxy. While it is technically possible for a child Helix Universal Proxy to also act as a parent Helix Universal Proxy, RealNetworks does not recommend this configuration due to the compounding of network and application latency.

> **Warning!** This feature is designed specifically for enterprise scenarios in which subnet traffic is routed through proxy software. Proxy routing is not recommended for use in any other scenarios, as the increased latency and administrative overhead are appropriate only to controlled network situations.

Rules for Routing

Each child Helix Universal Proxy directs its streams to other Helix Universal Proxys by use of rules.

Rules are sorted in the order in which they appear in Helix Administrator. Therefore, it makes sense to put the rules which affect the most requests later in the list. Put the most specific rules first.

Use an asterisk (*) to indicate a wildcard section. There are some conditions for using the wildcard:

- You can use only one asterisk per rule. For example, `*.example.com` is a valid entry in the **Routing Rule** box, but *.example.* is not. The following are all valid:

  `*` (forwards all requests to the Helix Universal Proxy shown in the list)
  `*.com` (forwards all requests that end in .com)
  `*.net`
  `*.example.com`
  `helixproxy.*.com`
  `helixproxy.example.*`
  `helixproxy.department.example.*`

- The asterisk cannot be used with a string. It can be used only within periods. Thus, `real*.example.com` is not valid.

Proxy Routing and Helix Universal Proxy Features

This section describes how proxy routing works with three of Helix Universal Proxy's features.

Pass-through

The pass-through feature under proxy routing works like this:

1. The client requests a stream through the child Helix Universal Proxy. The child Helix Universal Proxy forwards the request to the parent Helix Universal Proxy outside the subnet. The parent Helix Universal Proxy makes the request of the origin Helix Universal Server, which sends the data to the parent Helix Universal Proxy.
2. The child Helix Universal Proxy streams the request to the client.

The parent Helix Universal Proxy maintains the control connection to the origin Helix Universal Server; the child Helix Universal Proxy doesn't contact the origin Helix Universal Server directly.

Caching

With caching, the parent Helix Universal Proxy always forwards the requested media to the child Helix Universal Proxy; at the same time it stores the cache data itself. If a client requests the same data directly from the parent Helix Universal Proxy, that Helix Universal Proxy must still contact the origin Helix Universal Server before sending its cache. This prevents the parent Helix Universal Proxy cache from sending data that's out of date.

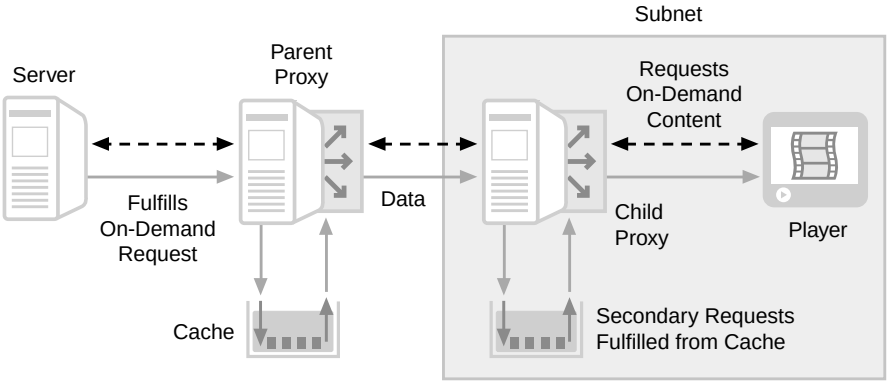
Each Helix Universal Proxy in proxy routing caches the requested media as it forwards the cache data to either another Helix Universal Proxy or to a client.

Caching under proxy routing works like this:

1. The client requests an on-demand stream, through the child Helix Universal Proxy. The child Helix Universal Proxy proxies the request and sends it to the parent Helix Universal Proxy outside the subnet. The parent Helix Universal Proxy makes the request of the origin Helix Universal Server. The origin server sends the data to the parent Helix Universal Proxy.
2. The parent Helix Universal Proxy caches the data and streams the request to the child Helix Universal Proxy.
3. The child Helix Universal Proxy caches the data and streams the request to the client.

Notice that the parent Helix Universal Proxy fills its cache with the data.

How Caching Works With Helix Universal Proxy Routing



Pull Splitting

The following steps describe proxy routing with the pull splitting feature:

1. The client requests a stream, through the child Helix Universal Proxy. The child Helix Universal Proxy proxies the request and sends it to the parent Helix Universal Proxy outside the subnet. The parent Helix Universal Proxy makes the request of the Helix Universal Server acting as the origin transmitter. Then, the server sends the data to the parent Helix Universal Proxy.
2. The child Helix Universal Proxy streams the data to the client.
3. The second client to request the same material from the child Helix Universal Proxy receives a split stream.

Notice that the splitting happens at the child level. A control connection is maintained with the origin transmitter, by way of the parent Helix Universal Proxy. Splitting does not happen at the parent Helix Universal Proxy; if a client connects to the parent Helix Universal Proxy and requests the same stream, the parent Helix Universal Proxy must proxy the request to the origin transmitter in the usual manner and splits that stream.

Customizing Proxy Routing Settings

When adjusting the proxy routing settings, you make changes to the child Helix Universal Proxy only. You do not need to make any changes to the parent Helix Universal Proxy.

➤ To set up proxy routing:

1. In Helix Administrator, click **Proxy Setup**. Click **Proxy Routing**.
2. In the **Routing Rules** area, click the "+" icon.

   A generic rule name appears.
3. In the **Edit Rule URL** box, type the rule information you want this child Helix Universal Proxy to use.
4. Click **Edit**.
5. If this rule points involves a parent Helix Universal Proxy (rather than simply allowing all requests that fit the rule to pass directly to an origin Helix Universal Server), use the following steps:
   a. From the **Use Parent Proxy** list, select `Yes`.
   b. In the **Parent Name** box, type the host name or the IP address of the parent Helix Universal Proxy where the client's request should be directed.
   c. In the **Parent RTSP Port** box, type the port number of the parent Helix Universal Proxy to which requests for RTSP should be directed.

      Match the parent Helix Universal Proxy's value for **RTSP Port** (usually `554`).
   d. In the **Parent PNA Port** box, type the port number of the parent Helix Universal Proxy to which requests for PNA should be directed.

      Match the parent Helix Universal Proxy's value for **PNA Proxy Port**, usually `1090`.
   e. In the **Parent MEI Port** box, type the port number of the parent Helix Universal Proxy to which cache requests should be directed.

      Match the parent Helix Universal Proxy's value for **MEI Port**, usually `7878`.
6. Repeat Step 2 through Step 5 for each rule that you will be adding.
7. If you didn't add the rules in the order described in "Rules for Routing", reorder them using the up and down buttons located next to the **Routing Table** box.
8. Click **Apply**.

Working With Redundant Proxies

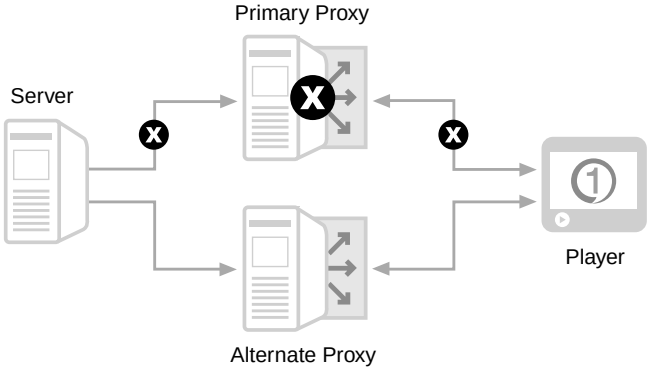
The redundant proxies feature enables you to add another level of redundancy to the delivery of your streaming media content. If an RTSP connection between RealOne Player and Helix Universal Proxy breaks, RealOne Player attempts to reconnect to the same Helix Universal Proxy.

However, if you have identified an alternate proxy, RealOne Player attempts to connect to the alternate proxy instead. You can have any number of alternate proxies defined. Alternate proxies work with both on-demand and live broadcasts.

Understanding Redundant Proxies

The redundant proxy feature enables real-time failover protection during both live and on-demand streaming media sessions for your clients. During the initial setup of the RTSP control channel, Helix Universal Proxy sends a list of alternate proxies for RealOne Player to use should there be a disconnection during playback. The disconnection can be the result of a failed network connection or a failed Helix Universal Proxy. When RealOne Player realizes the failure, it uses the alternate list provided by the primary Helix Universal Proxy to connect to an alternate Helix Universal Proxy. In the case where Helix Universal Proxy has provided multiple alternates, RealOne Player makes a random selection. The following illustration depicts a RealOne Player connecting to an alternate Helix Universal Proxy, after a failure of the primary.

Redundant Proxies



Setting Up Redundant Proxies

Setting up the redundant proxy feature requires that you identify alternates available to the primary Helix Universal Proxy. As a rule, alternates should be comparable to the primary Helix Universal Proxy:

- Alternates must have access to the same Helix Universal Servers as the primary Helix Universal Proxy.

  This allows alternates access to exactly the same content—whether live broadcasts or on-demand content—as the primary Helix Universal Proxy for which they are designated alternates.

- Alternates should have a similar configuration to the primary Helix Universal Proxy.

  For example, access control rules of an alternate should be similar to those of the primary proxy, to allow the same client access.

➤ To setup an alternate proxy:

1. In Helix Administrator, click **Proxy Setup**. Click **Redundant Proxies**.
2. In the **Alternate Proxies** box, click the "+" icon. A generic **Description** and **Port** appear. You can edit either value. Port must be the RTSP port for the alternate proxy. The description can be anything you like.
3. In the **Host** box, enter the host name or IP address of the alternate proxy.
4. Click **Apply**.

CHAPTER

8

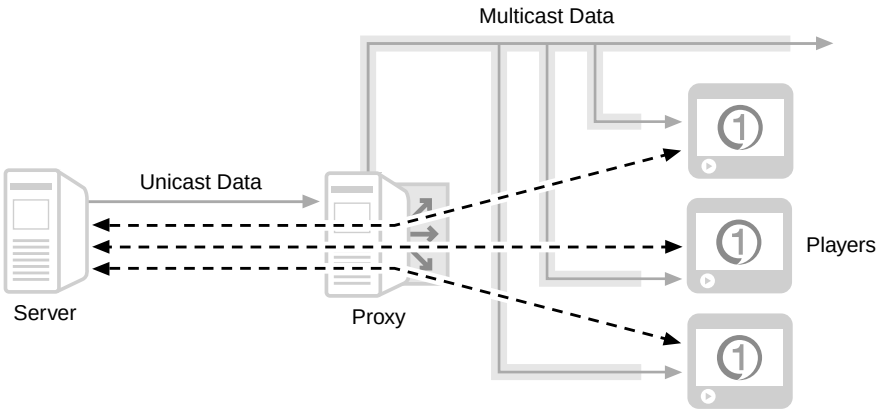
MULTICASTING

Multicasting helps you conserve bandwidth by reducing the number of live streams in use. It requires a specially configured network. You can multicast RealMedia, Windows Media, MPEG, and a number of RTP-based formats. Multicasting to the QuickTime Player is not available. In this chapter, you'll learn how to set up Helix Universal Proxy to multicast.

Overview

Multicasting is a way of sending a single live stream to multiple clients, rather than sending a stream to every single client. The players establish a data connection to the stream, rather than to the Helix Universal Proxy and to Helix Universal Server, as shown in the following illustration.

Multicasting



Helix Universal Proxy supports a form of multicasting called **back-channel multicasting**. In this method of multicasting, each media player maintains a control channel to Helix Universal Proxy and to Helix Universal Server. (The

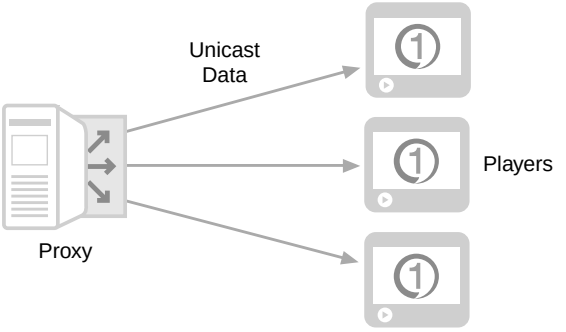
control channel is represented by the dashed lines in the illustration above.) A media player uses its channel to send commands such as **Stop**. The channel lets Helix Universal Proxy and Helix Universal Server receive a user name and password if authentication is used in either product. It also enables the Proxy Monitor described in Chapter 12 to track how many players are viewing the proxied multicast.

Back-channel multicasting works with all RealNetworks media players, including older players that use only the PNA protocol.

> **Note:** Since Helix Universal Proxy requires a control channel, it does not support scalable, one-way multicasting.

By contrast, regular unicasting transmission sends a stream to each client that requests it.

Unicasting



To take advantage of multicasting, both Helix Universal Proxy and clients, as well as the routers between them, must be multicast-enabled. For this reason, multicasting is mostly used with intranets where routers can be configured for multicasts. Multicast delivery can be performed over the Internet only where intermediary network devices have been multicast-enabled.

Multicast is automatically used (when available and configured) for pull-split streams. It is not used with pass-through or cache mode.

> **Note:** Helix Universal Proxy cannot broadcast using multicast to Windows Media Players.

Protocols Used for Multicasting

Multicasting uses the application-layer protocol RTSP to both send control information over a TCP channel to each client and to multicast live broadcast data to all clients over a UDP channel (or a TCP channel if UDP is unavailable.) Since multicasting is accomplished by RTSP for both control information and live data, it offers the following features:

- **Connection statistics**—Helix Universal Proxy can receive client connection information.
- **SureStream**—these multiply-encoded files are supported.

> **Note:** RTSP multicasting works only with RealSystem G2 and later clients.

Defining Multicasting

Before you set up multicasting, you need to do two things:

- Configure the network for multicasting.
- Select the addresses you'll use for your multicasts.

Setting Up the Network for Multicasting

Before setting up Helix Universal Proxy, verify the following items with your network administrator:

- Routers in your network are multicast-enabled.
- The computer running Helix Universal Proxy is correctly configured for multicast support.

In addition to network settings, clients must be configured to request multicast transmission of live material. Consult the client software's user guide for information on configuring the client.

As noted earlier, both Helix Universal Proxy and clients, as well as the routers between them, must be multicast-enabled in order for you to distribute presentations using the multicast features. This section describes only what is required to enable Helix Universal Proxy for multicast broadcasting.

Allocating Addresses and Port Numbers in Helix Universal Proxy

There are two factors to take into account when establishing the addresses and port numbers that Helix Universal Proxy will use for multicasting:

- Select addresses from a legal range of available addresses. Valid ranges are between 224.0.0.0 and 239.255.255.255. The network administrator should know which multicast addresses are available on your intranet. On the Internet, certain ranges such as the addresses between 224.0.0.0 and 224.0.0.255 are reserved for other uses; see RFC 1700, "Assigned Numbers" for a complete list of restricted addresses.
- You must select enough addresses for the type of file you are multicasting. See "Determining Required Addresses and Port Numbers" for information on selecting the appropriate number. You'll need to know how many bit rates are included in each file that you are multicasting, and set aside the appropriate number.

Although the information in this document will help you calculate the number of addresses and port numbers you'll need for multicasting, you'll still need to consult with your network administrator regarding the actual addresses you'll use.

Determining Required Addresses and Port Numbers

For each file that you are transmitting using multicast, you must calculate the number of addresses you'll need. The number of addresses is based on the number of bit rates in the file. For simple RealVideo files, figuring the number of addresses and port numbers is relatively simple. SureStream files are more complex, as they can contain several bit rates, each with its own number of streams.

Unless you can find out the number of bit rates in the files that you are streaming, you'll have to guess. A safe number is six bit rates per file; the maximum number of bit rates that would be present in a single SureStream file is 14, yet files prepared for multicasts are likely to include only the higher

encoding rates. A non-SureStream file would have at most one bit rate and two streams.

Addresses Needed for Back-Channel Multicasts

Bit Rates	Addresses
1	1
2	2
3	3
...	...
n bit rates	*n*

Configuring Back-Channel Multicasting

Follow the instructions below to set up Helix Universal Proxy for back-channel multicasting.

➤ To configure back-channel multicasting:

1. In Helix Administrator, click **Proxy Setup**. Click **Multicasting**.
2. In the **RTSP Port** box, type the port number to which Helix Universal Proxy will direct its RTSP multicast streams. The value in this box refers to the client's port number. A typical value is `554`.
3. Specify the range of addresses to which you want to multicast streams by filling in the **IP Address Range** box. Helix Universal Proxy uses the first available address in this range. If your multicast streams are referenced in SMIL files, you will need one address for each stream.

   Refer to "Determining Required Addresses and Port Numbers" to calculate the exact number of addresses you'll need.
4. Indicate how far multicast packets can travel over a network by typing a value in the **Time to Live** box. Each time a multicast data packet passes through a multicast-enabled router, its Time to Live is decreased by 1. When the value is decremented to 0, the router discards the data packet.

   The value for **Time to Live** can range from `0` to `255`. The larger the Time to Live, the greater the distance a data packet will travel.

The default value of 16 is enough to keep multicast packets within a typical internal network.

Time to Live (TTL) Values

TTL Value	Packet Range
0	Local host
1	Local network (subnet)
32	Site
64	Region
128	Continent
255	World

5. To allow missing packets to be resent to clients that request them, select Yes from the **Resend** list. This setting is optional. It adds some overhead to the traffic on your network; however, clients receive better quality multicasts.

6. Indicate which clients will be able to view your multicast presentations by configuring the user list.

   To require that clients with IP addresses in the user list must connect in multicast mode, set **Multicast Delivery Only** to Yes. When this is selected, those clients not configured for multicast will not be able to receive the multicast, and will receive an error message instead. Use this feature when you want to restrict the multicast to a limited number of clients, or if you are multicasting a high-bandwidth presentation and do not want unicast to be an option.

   a. Select Yes from the **Multicast Delivery Only** list.

   b. Click the "+" icon, and then in the **Edit Client Access Rule Number** box, type a rule number. The rule number is used by Helix Universal Proxy for sorting the address rules.

   c. Click **Edit**. The rule number is added to the **Client Access Rules** box.

   d. Type the IP Address of the client allowed to receive the multicast in the **Client IP Address** box. To allow any client to access the multicast, type Any.

   e. In **Client Netmask**, specify the range of client IP addresses around the one you entered in the preceding step by selecting a bit mask. If **Client IP Address** is set to Any, though, leave **Client Netmask** set to None. See

Appendix B for details about assigning a range of IP addresses using a bit mask.

Repeat Step b through Step e for each set of clients that will be accessing your multicast.

7. Click **Apply**.

Note: Access control rules are enacted before the user list rules. A client that is excluded by Access control will not be able to connect to any multicasts, regardless of the rules you create here. (IP access control is described in Chapter 10, "Access Control".)

CHAPTER

9

BANDWIDTH MANAGEMENT

Helix Universal Proxy uses several methods for managing bandwidth of streaming media. Whether you implement just one method, or you use several in conjunction, you have the ability to moderate the amount of streaming media traffic on your network.

Overview

When you install Helix Universal Proxy, the values for each of these settings is configured to use the maximum available number.

Techniques for managing the bandwidth you use include:

- **Maximum Client Connections**—limits the number of clients that can connect at one time.
- **Maximum Proxy Bandwidth**—restricts the bandwidth in use between Helix Universal Proxy and clients.
- **Maximum Gateway Bandwidth**—restricts the bandwidth in use between Helix Universal Proxy and Helix Universal Servers.

The default value for each method is 0, which means Helix Universal Proxy will use the maximum amount permitted by your license. If you establish values for all these features, Helix Universal Proxy will limit access when the lowest threshold is reached. If a client tries to make a request after a limit has been reached, the client receives an informative error message.

Maximum Client Connections

By using the **Maximum Client Connections** setting, you can limit the number of clients who connect simultaneously. Once this limit is reached, clients that attempt to connect receive an error message, and will not be able to connect until other clients disconnect.

➤ To limit access by limiting connections:

1. In Helix Administrator, click **Proxy Setup**. Click **Bandwidth Management**.
2. In the **Maximum Client Connections** box, type the number of client connections you want to allow simultaneously.

   This number can be from `1` to `32767`, as long as it is less than or equal to the number of streams permitted by your license. If it is `0` or blank, Helix Universal Proxy uses the number of streams specified by your license. The default value is `0`.
3. Click **Apply**.

Maximum Proxy Bandwidth

The **Maximum Proxy Bandwidth** setting establishes a threshold on the amount of bandwidth proxy uses for connections, in kilobits per second (Kbps). Helix Universal Proxy will make no new connections once this threshold has been crossed.

For example, if you set this to number to 100, and Helix Universal Proxy made one connection that used 80 Kbps, it can still make a connection of 40 Kbps even though the total Kbps in use is now 120. However, no new clients will be permitted to connect after that, as the maximum bandwidth use has been exceeded.

➤ To limit client bandwidth:

1. In Helix Administrator, click **Proxy Setup**. Click **Bandwidth Management**.
2. In the **Maximum Proxy Bandwidth** box, type the maximum number of kilobits per second (Kbps) that should be in use at once.

   For example, to limit the bandwidth to one megabit, specify maximum bandwidth usage by setting **Maximum Proxy Bandwidth** to `1024`.
3. When you have finished making changes, click **Apply**.

Maximum Gateway Bandwidth

You may want to limit the amount of bandwidth Helix Universal Proxy acquires, whether from another Helix Universal Proxy, Helix Universal Server, or the Internet.

Limiting gateway bandwidth limits the following Helix Universal Proxy functions:

- pass-through data connections
- pull splitter data connections
- initial cache requests

The number in **Maximum Gateway Bandwidth** is given in kilobits per second (Kbps). Helix Universal Proxy will make no new upstream connections once the gateway threshold has been crossed.

For example, if you set this to 2048, and Helix Universal Proxy made one connection that used 1024 Kbps, it can still make a connection of 1600 Kbps (even though the total Kbps in use is now 2624), but no new connections can be made after that.

➤ To limit Helix Universal Proxy-to-gateway bandwidth:

1. In Helix Administrator, click **Proxy Setup**. Click **Bandwidth Management**.
2. In the **Maximum Gateway Bandwidth** box, type the maximum number of kilobits per second (Kbps) that Helix Universal Proxy should use when it connects to its gateway.

   For example, to limit the bandwidth to two megabytes, specify maximum bandwidth usage by setting **Maximum Gateway Bandwidth** to `2048`.

3. When you have finished making changes, click **Apply**.

Limiting Access to Multicast Reception

By setting **Multicast Delivery Only** to `Yes` in the multicast list, you can require that clients within a certain range of IP addresses connect only in multicast mode. When this option is set to `Yes`, clients that are not able to connect in multicast mode receive an error message. If this option is `No`, clients that cannot connect in multicast mode can use unicast mode to receive the presentation.

This feature is described in Chapter 8, “Multicasting”.

CHAPTER

10

ACCESS CONTROL

Using the access control feature, you can limit access to media streams by clients, based on the IP address of the requesting machine and the Helix Universal Proxy port to which the request is made. This chapter explains how to implement this feature.

To implement user name and password control for media clients, use the authentication feature, which is described in Chapter 11.

Overview

The access control feature lets you associate permission to connect to certain Helix Universal Proxy ports with client addresses. For example, you could allow only certain groups in your organization to view clips routed by Helix Universal Proxy. You do this by listing their IP addresses, and the IP address of the machine on which Helix Universal Proxy is installed. If a client attempts to play a stream for which it hasn't been granted access, it will receive a message that the URL is not valid, or that the connection has timed out.

Additionally, you can restrict which clients can send requests to your Helix Universal Proxy by restricting access to the RTSP Proxy port (usually 554).

Helix Universal Proxy uses rules to implement access control policy. A rule consists of a client IP address or hostname, port value (or values), the Helix Universal Proxy IP address or hostname and an indicator for denying or allowing connections for that address/port pair.

Each rule has the following qualities:

- **Sorting Order**—Order in which a rule appears on the Access Rules list; determines the order a rule is implemented.
- **Description**—Descriptive statement of a rule.
- **Access Type**—Whether the client will be allowed or denied access.
- **Client IP Address or Hostname**—Client's address, or a range of addresses.

- **Client Netmask**—Client's netmask.
- **Server IP Address or Hostname**—Helix Universal Proxy's address.
- **Ports**—Port numbers on Helix Universal Proxy to which access is allowed or denied. These numbers correspond to settings on the Ports page: RTSP Port, PNA Port, and MMS Port.

Helix Universal Proxy implements the access rule numbers in order, from rules on the top of the Access Rules list, to the bottom. That is, the highest-placed rule will be enacted first, the lowest-placed last. This is important to keep in mind when establishing the order in which you wish your rules to apply.

Before using this feature, you must make decisions about the types of rules you will create. You can create as many rules as you like.

Access to Helix Administrator

When setting up access rules, it is important to note that you can inadvertently lock yourself out of the Admin Port. Therefore, the first rule you create should always be one that allows access to the Admin Port. This should be the third rule on the list, making it the third rule that Helix Universal Proxy implements in its access control policy. The steps for creating the Admin Port Access Rule are described in "Granting Access to Helix Administrator" on page 98.

Access Rule Methods

There are two general methods that you can use to restrict access to Helix Universal Proxy:

- specific address denial

  In this method, you deny access to a specific group of IP addresses and ports, and allow access to everyone else.

- specific address permission

  This method is the opposite of the preceding. Here, you allow access to a specific group of IP addresses and ports, and deny access to everyone else.

When you create a rule, you sort the rule's order on the `Access Rules` list using the up and down arrow buttons. Helix Universal Proxy uses the rule's order to determine the sequence in which the rule is carried out. You must create rules in a certain order for Helix Universal Proxy to execute rules properly.

When a client connects, it evaluates the connection starting with the first rule on the list. As soon as it finds a rule that matches the client's address, it allows or denies access according to the rule. As soon as Helix Universal Proxy finds a rule that matches the client's IP address, it allows or denies access, according to the rule.

When developing an access control policy, you should make the rules nearer the top of the list, the most strict. Reserve positions closer to the bottom for the most lenient rules.

The following table summarizes Helix Universal Proxy rules. The first two rules are predefined and should not be modified.

Helix Universal Proxy Rules

	Contents of Rules in Each Set	
Rule/Rule Set	Specific Address Denial	Specific Address Permission
`Allow all localhost connections`: Built-in rule. **Do not edit this rule.**	This rule permits access to Helix Universal Proxy from an application running on the same computer.	
`Deny connections to port 7070` : Built-in rule. **Do not edit this rule.**	This rule prevents other computers from accessing ports 7070, which is reserved for Helix Universal Proxy's use.	
Access to Helix Administrator	Clients permitted to use Helix Administrator. **Client IP address**: `Any` **Access**: `Allow` **Ports**: use value for *`Admin Port`*	
`Allow all other connections`: Specific client addresses This rule is also predefined, but you can edit it.	Clients **prevented** from accessing Helix Universal Proxy. **Client IP address**: specific client addresses. **Access**: `Deny` **Ports**: use values for specific ports	Clients **permitted** to connect to Helix Universal Proxy. **Client IP address**: specific client addresses. **Access**: `Allow` **Ports**: use values for specific ports
All other addresses	Clients **permitted** to use your Helix Universal Proxy. **Client IP address**: `Any` **Access**: `Allow` **Ports**: use values for content ports	Clients **prevented** from using Helix Universal Proxy. **Client IP address**: `Any` **Access**: `Deny` **Ports**: use values for specific ports This set of rules is optional.

Granting Access to Helix Administrator

The first step in creating rules is to set up a rule that enables you to connect to Helix Administrator, regardless of the restrictions you create in other rules. Although it appears that you are allowing everyone to access Helix Administrator, the only people who will use it are other administrators who know the Admin Port number (chosen randomly at installation) and who have a user name and password specifically for Helix Administrator.

> **For More Information:** To learn how to give access to Helix Administrator based on user name, see "Authenticating Helix Administrator Users" on page 105.

➤ To grant access to Helix Administrator:

1. If you do not know the Admin Port number, click **Proxy Setup>Ports** (or, in the **Access Control** page, click "**View assigned ports for this proxy.**") and note the value of the **Admin Port** field.
2. Click **Security>Access Control.**
3. Click the "+" icon in the **Access Rules** section.
4. In the **Edit Rule Description** box, type `AccessToAdmin`.
5. In the **Access Type** pull-down, select `Allow`.
6. In the **Client IP Address or Hostname** box, type `Any`. For additional security, type the IP address for users permitted to use Helix Administrator (separate multiple addresses with commas). To indicate a range of allowable addresses for this rule, select a bit mask from the **Client Netmask** drop down box. For more information on assigning a range of IP addresses using a bit mask, see Appendix B.
7. In the **Server IP Address** box, type `Any`.
8. In the **Ports** box, type the Admin Port number.
9. In the **Access Rules** area, click the up arrow to place `AccessToAdmin` as the third rule on the list.
10. Click **Apply**.

You will now be able to access Helix Administrator, no matter what rules you create in the next section.

Creating Specific Access Rules

Use the steps in this section to allow or deny access to specific IP addresses or address ranges.

> **Warning!** Be sure to first follow the steps in "Granting Access to Helix Administrator", or you will not be able to access Helix Administrator after you restart Helix Universal Proxy.

➤ To limit access according to IP number:

1. Review the port numbers in use. You'll use these in Step 8. In Helix Administrator, click **Proxy Setup>Ports**.

   Make a note of the values for **PNA Proxy Port** (usually `1090`) , **RTSP Port** (usually `554`), and **MMS Proxy Port** (usually `1755`).

2. In Helix Administrator, click **Security>Access Control**.

3. Click the "+" icon.

   A new rule appears at the bottom of the list, and a generic rule description appears in the **Edit Rule Description** box.

4. In the **Edit Rule Description** box, type a short description for the new access rule in the **Access Rules** list.

5. From the **Access Type** list, indicate whether permission is being granted or refused by selecting `Allow` or `Deny`.

6. In the **Client IP Address or Hostname** box, type the IP address of the client machine. To indicate a range of addresses, select a bit mask from the **Client Netmask** drop down box. For more information on assigning a range of IP addresses using a bit mask, see Appendix B.

   > **Tip:** To refer to all clients, regardless of IP address, type the word `Any` in the **Client IP Address** box, and leave the **Client Netmask** box set to None.

7. In the **Server IP Address or Hostname** box, type the IP address or host name of the client machine or network card.

   You can type a specific address, or use the word `Any` to refer to any IP address Helix Universal Proxy uses to listen for incoming requests.

If you type a specific IP address or host name, rather than the word `Any`, you must also add that address to the IP Binding list. See "Binding To An IP Address" for more information.

8. Finally, list the Helix Universal Proxy port numbers to which you want to restrict access. In the **Ports** box, type the port numbers you noted in Step 1, separated by commas. For example, type `1090, 554`.

   To restrict access to all Helix Universal Proxy ports, the port numbers should match the other port numbers you've instructed Helix Universal Proxy to listen to; look at the port numbers for RTSP port, PNA port, HTTP port, MMS Port

9. Click **Apply**.

CHAPTER

11

AUTHENTICATION

Helix Universal Proxy authentication provides a way for you to control what or who can access your Helix Universal Proxy, a colleague perusing Helix Administrator, or a user requesting content streamed by Helix Universal Proxy. With this feature, you can configure Helix Universal Proxy to require a valid user name and password before allowing a client to access a particular URL.

To limit visitors to Helix Universal Proxy via bandwidth, connection volume, or IP address, use the methods described in Chapter 9 and Chapter 10.

Overview

Authentication verifies the identity of users that send requests to Helix Universal Proxy. The verification comes in the form of asking for a name and password. To receive requests on behalf of clients, Helix Universal Proxy requires an accounting channel between the requesting client and itself. Helix Universal Proxy uses the accounting channel to request and receive authentication information.

You can require authentication for:

- **Administrators** —Allow certain people in your organization to use Helix Administrator. To protect changes to your Helix Universal Proxy by unauthorized users, Helix Universal Proxy is installed with authentication enabled for Helix Administrator access.
- **Individual users**—An additional database can be used to list all potential content users, content sites all users can view, and what type of access they have. Several additional options are available for this type of authentication.

Authentication is a feature also used by some Helix Universal Servers. As a result, some users may be asked more than once for a user name and password—once by Helix Universal Proxy, and once by the Helix Universal Server. In each case, a username and a password is determined as stored by that particular Helix Universal Proxy and Helix Universal Server.

Compatible Client Versions

RealPlayer versions 3 and earlier do not work with authentication and may display an error message. RealPlayer 4 through RealOne Player supports user authentication.

When to Use Authentication

The following are factors in deciding to use this feature:

- You want to restrict user access to content originating from specific locations.
- You want to ensure that only certain users can play streaming media that originates outside your network.
- You want to limit access to content Helix Universal Proxy streams using a more specific method than noting the client's IP address. (The access control list enables access based on the client's address.)
- You want to collect data from users before they play streamed content. (Collecting data is not necessarily part of authentication; it is just something you can require if you implement authentication.)
- You want to track how much time specific users are playing certain clips.

Understanding Authentication

The authentication feature uses two main components to validate user information and check associated permissions:

- Databases
- Realms

You must use databases and realms to require authentication in both Helix Universal Proxy areas: for Helix Administrator users, and for individual users requesting content.

Databases

Authorized users (administrators or users making media requests) are stored in separate databases. Helix Universal Proxy uses a flat file database structure in its default configuration. For large-scale implementations of authentication, Helix Universal Proxy supports ODBC and MS SQL-compliant, and mSQL databases.

The following table explains the flat file databases automatically installed with Helix Universal Proxy.

Default Databases

Database Name	Contents	Purpose of the Contents
Admin_Basic	User names and passwords for Helix Administrator users.	By default, Helix Universal Proxy uses this database to validate user names and passwords used to access Helix Administrator.
Content_RN5	User names and passwords for content users; added upon first use.	Helix Universal Proxy uses this database to validate users trying to access secured content.

Note: Refer to "Authentication Data Storage" on page 187 for details on the database structure.

Authentication Realms

Authentication realms provide a way to associate databases with a protocol to encrypt their username, passwords, and other information. When you configure a realm, you associate a database with this realm and Helix Universal Proxy references this database to verify a user's credentials.

When you create or edit a realm, you specify the following information:

- An authentication protocol for encryption of user names, passwords, etc.
- An associated database containing user information
- A realm description
- A realm ID

  The default realms conform to the following format:

  proxyname.RealmId

You do not have to use this convention, but you must include a period (.) in the realm ID or the realm will not work properly.

The installation process automatically creates the following authentication realms. The following table explains these realms, and their default settings on Helix Universal Proxy:

Existing Realms and Their Default Settings

Realm	Decription	Realm ID	Protocol	Database
SecureAdmin	Used to authenticate Helix Administrator users.	*proxyname*.AdminRealm	Basic	Admin_Basic
ConnectRealm	Used to authenticate proxy users.	*proxyname*.ConnectRealm	Basic	Content_RN5

Authentication Protocols

Authentication protocols determine the password encryption method used by Helix Universal Proxy. The proxy supports three protocols for encrypting user passwords:

- **Basic**—encodes the user's name and password with the Base64 algorithm and sends it to Helix Universal Proxy, which then decodes the password and verifies it. This protocol sends the user's password over the network or public Internet in a simple manner.
- **RealSystem 5.0**—also called *RN5*, is RealNetworks' own encryption protocol, developed for RealServer version 5. If your material will be served to users working with RealNetworks players from version 5 and up, use this authentication protocol. This is a more sophisticated protocol than Basic authentication. For RealNetworks player versions earlier than 5, you must use the basic protocol for backwards compatibility. The earlier versions of RealNetworks players will not work with this protocol.
- **Windows NT LAN Manager**—this method enables Helix Universal Proxy to use the existing Windows NT or Windows 2000 database of users and groups. It also allows access control of content via NTFS file permissions.

  When using NTLM authentication, you need to be aware of the following:

  - All users accounts must exist on the local NT computer. NTLM authentication will not work with accounts on other servers within the domain except accounts on a domain server. In this case, you'll

need to use the username input value in the form, `domainname\username`.

- You add all user accounts through the Windows NT User Manager.
- The built in guest account is not available for use in authentication.
- When you select NTLM authentication in Helix Administrator, if you do not specify a user group, all groups are authenticated.
- Blank passwords are not supported.

Note: This method is only available to systems using Windows NT, and Windows 2000 and requires that Helix Universal Proxy itself be installed on the Windows NT or Windows 2000 machine.

Authenticating Helix Administrator Users

At installation, Helix Universal Proxy is configured to prompt for a user name and password for a Helix Administrator user. As stated earlier, the information you enter is added to the `Admin_Basic` database which is associated with the `SecureAdmin` realm.

Helix Universal Proxy identifies incoming requests to access Helix Administrator by the protected path `/admin` that is in the URL request. It automatically prompts for a user name and password and verifies them against the information in the `SecureAdmin` realm that points to the `Admin_Basic` database.

You'll need to make informed decisions when modifying the `SecureAdmin` realm. Doing otherwise can remove your access to Helix Administrator.

➤ **To add user names for Helix Administrator authentication using the supplied realm:**

1. In Helix Administrator, click **Security>Realms**.
2. In the **Authentication Realms** list, select `SecureAdmin`.
3. Click **Add a User to Realm**.
4. In the new window that appears, type the user's name in the **Name** box.
5. In the **Password** box, assign a password.
6. In the **Confirm Password** box, type the password again.

7. Click **Okay**. A message appears; click **Close Window**.

> **Tip:** Optionally, you can set up a separate database and realm from the one supplied by Helix Universal Proxy during installation. In this case, refer to "Authenticating Users Requesting Content" on page 106.

Authenticating Users Requesting Content

You need to set up Helix Universal Proxy if you decide to authenticate users trying to access Helix Universal Proxy to deliver either on-demand or live content. When you set up and customize authentication, you must perform the necessary steps in the correct order or authentication will not work. As you are planning your authentication model, remember the DRA (Database-Realm-Authentication) method:

1. **Database:** First, you must either create a new database, or you must add or verify an existing database in Helix Universal Proxy.
2. **Realm:** Next, you need to create or use an existing authentication realm pointing to an existing database. Then, add users to this database, (or use a pre-populated one.)
3. **Authentication:** Finally, you need to enable the feature, and choose a specific realm and database to authenticate users. Optionally, you can
   - Identify those sites for which Helix Universal Proxy will not require authentication
   - Allow users to view the same content from more than one site

Setting up Databases

Step 1: Optionally, Create a New Database

Helix Universal Proxy includes templates for common database formats. To learn more about database structure and how to use Helix Universal Proxy's database templates, refer to "Understanding Authentication Data" on page 187.

Step 2: Verify or Add Your Database in Helix Universal Proxy

Any database that contains user information that you want Helix Universal Proxy to use to validate credentials must exist in the Helix Universal Proxy

database list. If you plan to use the default flat file database, you simply need to verify that the setup procedure created this database and it exists in Helix Universal Proxy's database list. If you are using an ODBC, MS SQL or mSQL database, you must add it to the Helix Universal Proxy database list.

➤ To verify a default database:

1. In Helix Administrator, select **Security>User Databases**.
2. Select an existing database.
   - To use the default connection database, in the **Databases** list, verify that the `Connect_RN5` database appears.

➤ To add a new database:

Use the instructions below to choose the name and type of database that will store users' names and passwords.

> **Note:** If you're using an ODBC or mSQL database, refer to "Setting Up Other Types of Data Storage" on page 192 in Appendix C to ensure you've correctly configured your database before you add it to Helix Universal Proxy.

1. In Helix Administrator, select **Security>User Databases**.
2. Click the "+" icon and type the database name in the **Edit Database Name** box.
3. From the **Database Type** list, select the appropriate data storage method: flat file, ODBC, or mSQL.
4. Depending on the database type method you chose, additional information is required.

   Flat File needs only the path to the main text file directory. For example, the `con_r_db` directory under the main Helix Universal Proxy directory. See "Understanding Authentication Data" on page 187.

   mSQL has two required names, and three optional items:

   - **Host Name**—IP address or DNS name of computer where database is stored. (Required field.)
   - **Database Name**—Name of the database. (Required field.)
   - **Table Name Prefix**—Prefix used to make field names unique, when used with an existing database. (Optional field.)

- **User Name**—Name required by database application. (Optional field.)
- **Password**—Password required by database application. Re-enter your password in the **Confirm Password** box to ensure you typed it correctly. (Optional field.)

ODBC uses the same information as mSQL, but ODBC does not ask for a Host Name. (Refer to "Setting Up Other Types of Data Storage" on page 192 for further instructions.)

5. After filling out the appropriate values, click **Apply**.

Setting up Realms

A realm contains information about the type of authentication protocol and the database where the authenticated users' names will be stored. To set up a realm for Helix Universal Proxy users, you can either use the default realm `ConnectRealm`, or you can create a new one.

➤ To use the default realm, `ConnectRealm`:

1. In Helix Administrator, click **Security**>**Realms**.
2. Browse, add usernames and passwords. Refer to "Working with User Names and Passwords" on page 112.

➤ To create a new realm:

1. In Helix Administrator, click **Security**>**Realms**.
2. Click the "+" icon and enter a name for this realm in the **Edit Realm Description** box.
3. In the **Realm ID** box, type a name. You will use this name in other areas of Helix Administrator, so make a name that is meaningful to you. The Realm name may also appear to users as part of the name and password prompt.
4. In the **Authentication Protocol** list, select the authentication method you want to use for this realm:

Helix Universal Proxy has three methods of authenticating the identity of visitors. Each realm can use only one authentication method.

- **Basic**—encodes the user's name and password with the Base64 algorithm and sends it to Helix Universal Proxy, which then decodes the password and verifies it. You will also need to select a database in which the names

and passwords of authenticated users will be stored; refer to "Setting up Databases" on page 106.

- **RealSystem 5.0**—also called "RN5", it is RealNetworks' own authentication protocol. This is a more sophisticated protocol than Basic authentication. It provides better security than Basic because it does not send the password in a manner that can be reversed.

  You will also need to select a database in which the names and passwords of authenticated users will be stored; refer to "Setting up Databases" on page 106. In addition, these passwords are encrypted. To change them, refer to "Changing RealSystem 5.0 Authentication Passwords" on page 114.

- **Windows NT Lan Manager**—this method allows Helix Universal Proxy to use an existing Windows NT database of user groups and permissions. You do not need to select a database—instead, Helix Universal Proxy will use the NTLM list of names. This protocol uses Windows NTLM authentication.

  This method is only available to systems using Windows NT, Windows 2000 and requires that Helix Universal Proxy itself be installed on either a Windows NT or Windows 2000 Server. For authenticating content, it also requires a Web browser and RealNetworks RealOne Player or RealPlayer.

  Use the additional steps shown here:

  a. Type the appropriate provider in the **Provider** list, such as `NTLM`.
  b. Optionally, type the Group name in the **Group** box
  c. Click **Apply**.

Complete these last three steps if you're using **Basic** or **RealSystem 5.0** as an authentication protocol.

5. In the **Database** list, select the database you want to use for this realm.
6. Browse, add usernames and passwords. Refer to "Working with User Names and Passwords" on page 112.
7. Click **Apply**.

Setting up Authentication

To set up authentication in Helix Universal Proxy, you need to turn on the feature, and decide which realm and database to use with authentication.

Optionally, you can select sites all users are allowed to visit and allow users to view content from more than one location.

Step 1: Enable the Authentication Feature.

➤ To enable authentication:

1. In Helix Administrator, click **Security>Authentication**.
2. From the **Enable Authentication** list, select `Yes`.

Step 2: Select a Specific Realm

➤ To pick a realm:

- From the **Realm** list, select `ConnectRealm`.

  If you have set up another Realm, select that name here.

Step 3: Select a Specific Database

➤ To choose a database:

- From the **Database** list, select `Connect_RN5`.

  If you have set up another database, select that name here. If the realm you selected is using Windows NTLM as an authentication protocol, select **None**.

Step 4: Optionally Identify Permitted Sites

In this step you choose the sites which all users are allowed to visit without having to supply a user name and password.

➤ To set up permitted sites:

1. In the **No-Authenticate Rules** area, click the "+" icon. A generic rule name appears.
2. In the **Edit Rule Name** box, type a name for this rule.
3. Click **Edit**.

4. In the **Host** box, type the name of the site to which all users will be permitted access. Use a single asterisk to avoid specificity..

Naming Scheme for Host

Use this form...	...to indicate these sites:
*.org	All sites ending with .org
example.com	The site named www.example.com,
*.example.com	Will include www.sports.example.com among others.

Note: Use only one asterisk. For example, `*.*.com` is not allowed.

5. Click **Apply**.

Step 5: Optionally Allow Users to Log On From Multiple Locations

If you want a user to be able to use more than one client and view content from more than one location, set **Allow Duplicate IDs** to `Yes`. You can also use this option as a method of limiting access to groups. For example, you could set **Allow Duplicate IDs** to `Yes` and assign all marketing employees one user name and password, then the entire department could then use this account to view content.

Normally, when **Allow Duplicate IDs** is set to `No`, a user can view a given clip from only one computer at a time. If a user tries to log in from a second computer and view the same content, he or she will receive an error message. The user must log out at the first location before being permitted to log in at the second location. Users will still be able to view different content even though they are logged in at different locations.

➤ To allow users to view a clip from more than one location or to permit more than one person to use a single account:

1. In Helix Administrator, select **Security**>**Authentication**.
2. From the **Allow Duplicate IDs** list, select `Yes`.
3. Click **Apply**.

Working with User Names and Passwords

Use the following instructions to manage the list of authorized users for any type of authentication.

Adding a User

If you are adding a user to a new database, you must add that database and associate it with the proper realm using Helix Administrator before you add a user to realm. Refer to "Setting up Databases" on page 106 for more information.

> **Note:** If you are using Windows NTLM to manage the list of users, passwords, and groups, use Windows NT User Manager or other utilities instead of the instructions below.

➤ To add a user name and password:

1. In Helix Administrator, click **Security**>**Realms**.
2. In the **Authentication Realms** list, select the name of the realm to which you want to add a user:
   - For Helix Administrator users, select `SecureAdmin`.

     If you have set up another Realm for this purpose, select that name here.
   - For users requesting a connection, select `ConnectRealm`.

     If you have set up another Realm, for this purpose, select that name here.
   - For any other category of authentication, select the name of the realm. (To learn more about realms, see "Setting up Realms" on page 108.)
3. Click **Add a User to Realm**.
4. In the new window that appears, type the user's name in the **Name** box.
5. In the **Password** box, supply the user's password. Passwords are case-sensitive. RealNetworks recommends following good password practices:
   - Avoid common words that are easy to guess.
   - Do not use a word associated with the user, such as a first name.
   - Do not use the same password for multiple users.

- For highest security, use a random combination of letters and numbers in different cases.

  Tip: Keep track of the passwords you assign. Helix Administrator allows you to change passwords, but not to look them up.

6. In the **Confirm Password** box, type the password again.
7. Click **OK**.

Removing a User

The following procedure explains how to delete a user from a database. Helix Administrator does not have a bulk delete feature.

➤ To remove a user:

1. Click **Security>Realms**.
2. In the **Authentication Realms** list, select the name of the realm in which you want to delete a user. The predefined realms are described in "Setting up Realms" on page 108.
3. Click **Remove a User from Realm**.
4. In the new window that appears, enter the user's name in the **Name** box.
5. Click **OK**.

Browsing All User Names

The browsing feature lists all user names defined for an authentication realm.

➤ To browse all users:

1. Click **Security>Realms**.
2. In the **Authentication Realms** list, select the realm you want to browse. The default realms are described in "Setting up Realms" on page 108.
3. Click **Browse Users in Realm**. The pop-up window lists all user names defined for that realm.

Changing a Password

The following procedure explains how to change the password for an existing user. The Helix Administrator interface does not allow you to look up existing passwords.

➤ To change a password:

1. Click **Security>Realms**.
2. In the **Authentication Realms** list, select the name of the realm that contains the user. The predefined realms are described in "Setting up Realms" on page 108.
3. Click **Change User Password**.
4. In the new window that appears, enter the user's name in the **Name** box.
5. In the **Password** box, specify the user's new password.
6. In the **Confirm Password** box, type the password again.
7. Click **OK**.

Changing RealSystem 5.0 Authentication Passwords

When you use the RealSystem 5.0 authentication protocol, Helix Universal Proxy stores all passwords in an encrypted format. Passwords can be entered and changed through Helix Administrator. If you want to change the passwords manually, without using Helix Administrator, you can use the supplied password command line utility `mkpnpass`. It is located in the Helix Universal Proxy `Bin` directory.

You can also use these instructions as a basis for writing your own CGI scripts and Web pages to accomplish the same purpose automatically.

➤ To use the password tool manually:

1. At a command line, in the Bin directory, type the following:

   `mkpnpass` *username realm*

   where:

   username is the user name exactly as it is entered and will be stored in the authentication database or text file.

   realm is the value of the `Realm` variable specified in the relevant list.

For Helix Administrator users, use the value of the `Realm` variable in the `RealAdministrator_Files` list within the `FSMount` list in the configuration file. (You must open the configuration file itself to see this value.)

2. A password prompt appears, followed by a prompt to type the password again.

   The resulting encrypted password is displayed on the screen.

   Helix Universal Proxy encrypts passwords with the MD5 hashing algorithm. It uses the form `MD5("`*username:realm:new_password*`")`. On BSD systems and some other UNIX systems, you can generate these passwords with the following command:

   ```
   echo -n "username:realm:new_password" | md5
   ```

3. Add the resulting encrypted password into the appropriate field of the database:

   - For flat text files, place it in the password field of the `User` directory (see "Users Directory").
   - For databases, place it in the password field of the Users table (see "Users Table").

CHAPTER

12

PROXY MONITOR

You can monitor the volume of inbound traffic, and view the number of clients currently connected. This chapter provides brief instructions on the proxy monitor feature.

To generate reports of historical activity, see Chapter 13, "Access and Error Logs".

Viewing Helix Universal Proxy Activity

Helix Administrator includes a section where you can view Helix Universal Proxy activity.

➤ To view Helix Universal Proxy activity using Helix Administrator:

In Helix Administrator, click **Logging & Monitoring**, then click **Proxy Monitor**. The monitor page appears in the right-hand frame. It dynamically updates to show information about the number of connections, and so on.

Additional information about the information shown is available on the monitor page itself.

Monitor in Helix Administrator

The significance of these numbers is shown below:

- **Connected Clients**—shows how many clients are currently using Helix Universal Proxy.
- **Total Clients Served**—gives the number of clients that have used Helix Universal Proxy since it was last started.
- **Data Source**—shows the Helix Universal Proxy features used to deliver the requests.
- **Client Traffic**—lists the number of clients whose requests were delivered using the particular Data Source method, in bits per second.
- **Gateway Traffic**—shows the amount of bandwidth consumed by each Data Source type, in bits per second.

CHAPTER
13

ACCESS AND ERROR LOGS

This chapter explains how Helix Universal Proxy records information about client connections and other events. Using the log files, you can compile reports about system activity, gathering the statistical information you need.

> **Tip:** If you're interested in designing custom reports to track specific activities on Helix Universal Proxy, refer to Chapter 14.

Understanding Log Files

Helix Universal Proxy maintains an access log that includes statistics about client connections. It keeps another log of error and informational messages about Helix Universal Proxy operation. The log files are text files that you can open with any text editor, or parse with a script or application. As accesses or errors occur, Helix Universal Proxy appends information to the end of the appropriate log file. The following sections introduce you to the log files and their features.

Access Log

The access log records information about requests by RealNetworks media players, Windows Media Player, and QuickTime Player. Using these logs, you can find out what clips were played, the times when media players connected, and so on. This information can help you determine which clips are most popular, for example.

The default access log is `proxy.log`, which is located in the `Logs` subdirectory of the main Helix Universal Proxy installation directory.

Logged Information

Helix Universal Proxy provides six logging styles that determine the amount of information gathered on each access attempt. In general, each style builds on

the preceding style, adding more information. For instance, logging style 0 gathers the least amount of information. Logging style 1 includes the style 0 information, and adds more information, and so forth. You choose just one logging style for the entire log.

> **For More Information:** The section "Access Log File Format" on page 121 explains the logging styles and information fields.

Media Player Statistics

All logging styles can record statistics about a media player's playback experience. These statistics let you learn how many media packets were dropped, for instance, or whether the viewer paused the clip. There are four types of client statistics. You can use any combination of these statistics types, up to all four. Or, you can turn off client statistics gathering entirely. As well, users may choose not to report statistics.

> **For More Information:** See "Client Statistics" on page 132.

Error Log

The error log contains information and error messages about Helix Universal Proxy operation. By looking for patterns of errors, you can troubleshoot and correct possible problems on your site. The default file name is `proxyerr.log`, and the file is generated in the `Logs` subdirectory of the main Helix Universal Proxy installation directory. Helix Universal Proxy records an entry in this log only when an error occurs. Until an error happens, the file does not exist. The error log uses the following syntax:

```
***date time proxyname(process_ID): error_message
```

The following table explains these fields in the error log file.

Error Log Fields

Entry	Meaning
`***`	Three asterisks indicate an error. Informational messages are not preceded by asterisks.
`date`	Date on which the error occurred, given in the form `dd-Mmm-YY`, as in `26-Apr-02`.
`time`	Time the error occurred on the Helix Universal Proxy clock, given in the form `HH:MM:SS.xyz`, as in `21:05:10.614`.

(Table Page 1 of 2)

Error Log Fields (continued)

Entry	Meaning
proxyname(process_ID)	Helix Universal Proxy name, followed by the process ID in parentheses.
error_message	Text of the message.

(Table Page 2 of 2)

Note: If you receive a message that refers to a fatal error, contact the RealNetworks Technical Support Department for assistance.

Log File Rolling

The access and error log files can grow indefinitely as they accumulate data. To keep log files manageable, you can limit a log file to a specific size. With the access log, you can also create a new log at a preset interval, such as every six hours or two weeks, depending on the amount of data you expect to log. Helix Universal Proxy begins, or *rolls*, a new log file when the limit is reached. Rolled log files are named with the following format:

file_name.log.*timestamp*

The name and extension are set through Helix Administrator, as described in "Customizing the Access and Error Logs" on page 139. The timestamp has the following format, using a 24-hour clock:

YYYYMMDDHHMMSS

For example, the following file was created on June 22, 2002, at 1:49.53 P.M:

proxy.log.20020622134953

Access Log File Format

Helix Universal Proxy records each access request in a separate record written to a new line in the access log. Fields within a record are separated by spaces or by pipes (|). One record is created for every clip served. If the client requests a presentation that includes several clips, one record is created for each clip in the presentation.

Logging Style

Helix Universal Proxy provides six logging styles, numbered 0 through 5. Styles 1 through 4 each include the information of lower logging styles. For

example, style 3 collects the same information as styles 0, 1, and 2, as well as some additional information. The default is style 5, which adds a `presentation_ID` field to the information in style 2. The following sections describe which fields each logging style collects. The section "Access Log Fields" on page 124 explains the information logged in each field.

> **Tip:** Although square brackets in syntax typically indicate optional material, the square brackets shown in the following access log syntax actually appear in the access log records.

> **Note:** In the following examples, client statistics are not logged, so each entry shows `[UNKNOWN]` where the statistics fields would be. If you collect client statistics, therefore, each log entry will contain additional information. For more information, see "Client Statistics" on page 132.

Logging Style 0

Logging style 0 uses this format:

```
client_address - - [timestamp] "GET filename protocol/version" HTTP_status_code
bytes_sent [client_info] [client_stats_results] [proxy_info]
```

Here is an example of an actual log record, showing that 858,636 bytes of the requested clip were sent over RTSP:

```
207.188.7.125 - - [26/Jun/2002:10:31:44 -0700] "GET real9video.rm RTSP/1.0"
200 858636 [WinNT_5.0_6.0.10.714_RealPlayer_RN92PD_en_686] [UNKNOWN]
[Demand Cache Hit]
```

Logging Style 1

Logging style 1 follows this format:

```
client_address - - [timestamp] "GET filename protocol/version" HTTP_status_code
bytes_sent [client_info] [client_stats_results] file_size file_time sent_time
resends failed_resends [proxy_info]
```

The following sample log record shows the same information as logging style 0, but adds information on file size, clip timeline length, actual time streamed, and resent packages:

```
207.188.7.125 - - [26/Jun/2002:10:06:33 -0700] "GET real9video.rm RTSP/1.0"
200 858636 [WinNT_5.0_6.0.10.714_RealPlayer_RN92PD_en_686] [UNKNOWN]
926322 217205 1 0 [Demand Cache Hit]
```

Logging Style 2

This is the format for logging style 2, which is identical to style 1, except that it records a global client ID.

```
client_address - - [timestamp] "GET filename protocol/version" HTTP_status_code
bytes_sent [client_info] [client_ID] [client_stats_results] file_size file_time
sent_time resends failed_resends [proxy_info]
```

Here is an example:

```
207.188.7.125 - - [26/Jun/2002:10:07:42 -0700] "GET real9video.rm RTSP/1.0"
200 858636 [WinNT_5.0_6.0.10.714_RealPlayer_RN92PD_en_686]
[8e07b707-19b7-448b-96b6-96c90151f2a6] [UNKNOWN] 926322 217 205 1 0
[Demand Cache Hit]
```

Logging Style 3

Logging style 3 follows this format. It builds on style 2 by adding information about the streams and the Helix Universal Server or parent Helix Universal Proxy that delivered the clip:

```
client_address - - [timestamp] "GET filename protocol/version" HTTP_status_code
bytes_sent [client_info] [client_ID] [client_stats_results] file_size file_time
sent_time resends failed_resends [stream_components] [start_time]
server_address [proxy_info]
```

This example shows the origin server and stream information added to the end of the record:

```
207.188.7.125 - - [26/Jun/2002:10:09:09 -0700] "GET real9video.rm RTSP/1.0"
200 858636 [WinNT_5.0_6.0.10.714_RealPlayer_RN92PD_en_686]
[8e07b707-19b7-448b-96b6-96c90151f2a6] [UNKNOWN] 926322 217 205 1 0
[1 1 0 0] [26/Jun/2002:10:05:14] 208.147.89.157 [Demand Cache Hit]
```

Logging Style 4

Logging style 4 adds information about the clip's average bit rate and number of packets sent:

```
client_address - - [timestamp] "GET filename protocol/version" HTTP_status_code
bytes_sent [client_info] [client_ID] [client_stats_results] file_size file_time
sent_time resends failed_resends [stream_components] [start_time]
server_address average_bitrate packets_sent [proxy_info]
```

Here is an example:

```
207.188.7.125 - - [26/Jun/2002:10:10:04 -0700] "GET real9video.rm RTSP/1.0"
200 858636 [WinNT_5.0_6.0.10.714_RealPlayer_RN92PD_en_686]
[8e07b707-19b7-448b-96b6-96c90151f2a6] [UNKNOWN] 926322 217 205 1 0
[1 1 0 0] [26/Jun/2002:10:05:14] 208.147.89.157 34816 488 [Demand Cache Hit]
```

Logging Style 5

Logging style 5, which is the default style, does not build on the preceding styles. Instead, it copies style 2 and adds a presentation ID that helps you keep track of presentations that contain multiple clips:

```
client_address - - [timestamp] "GET filename protocol/version" HTTP_status_code
bytes_sent [client_info] [client_ID] [client_stats_results] file_size file_time
sent_time resends failed_resends presentation_ID [proxy_info]
```

The following is an example of a logging style 5 entry:

```
207.188.7.125 - - [26/Jun/2002:10:11:03 -0700] "GET real9video.rm RTSP/1.0"
200 858636 [WinNT_5.0_6.0.10.714_RealPlayer_RN92PD_en_686]
[8e07b707-19b7-448b-96b6-96c90151f2a6] [UNKNOWN] 926322 217 205 1 0 124
[Demand Cache Hit]
```

Access Log Fields

The following table summarizes the various logging fields that may appear in an access record, and indicates which logging styles include the fields. The following sections describe the access log fields in detail.

Access Log Fields

Log Field	Logging Styles	Reference
client_address	0, 1, 2, 3, 4, 5	page 125
[timestamp]	0, 1, 2, 3, 4, 5	page 125
"GET filename protocol/version"	0, 1, 2, 3, 4, 5	page 125
HTTP_status_code	0, 1, 2, 3, 4, 5	page 126
bytes_sent	0, 1, 2, 3, 4, 5	page 126
[client_info]	0, 1, 2, 3, 4, 5	page 126
[client_ID]	2, 3, 4, 5	page 127
[client_stats_results]	1, 2, 3, 4, 5	page 128
file_size	1, 2, 3, 4, 5	page 128
file_time	1, 2, 3, 4, 5	page 128

(Table Page 1 of 2)

Access Log Fields (continued)

Log Field	Logging Styles	Reference
sent_time	1, 2, 3, 4, 5	page 128
resends	1, 2, 3, 4, 5	page 128
failed_resends	1, 2, 3, 4, 5	page 128
[stream_components]	3, 4	page 129
[start_time]	3, 4	page 129
server_address	3, 4	page 129
average_bitrate	4	page 129
packets_sent	4	page 129
presentation_ID	5	page 129
proxy_info	1, 2, 3, 4, 5	page 130

(Table Page 2 of 2)

Client Address

The client_address field gives the IP address of the client, such as 123.45.123.45. Following the IP address are two hyphens for compatibility with standard Web server log formats.

Timestamp

The [timestamp] field indicates the time that the client accessed the file according to the Helix Universal Proxy clock. It uses the following format:

```
[dd/Mmm/yyyy:hh:mm:ss TZ]
```

Here, TZ is the time zone expressed as the number of hours relative to the Coordinated Universal Time (Greenwich, England). For example:

```
[26/Jun/2002:10:10:04 -0700]
```

File Name and Protocol

The "GET filename protocol/version" field lists the file name and path requested by the client. The path is everything in the URL after the port number. If the client requests a file that doesn't exist, UNKNOWN appears in place of the file name. Possible values for the application-layer protocol used to send the clip to the client are RTSP, PNA, and MMS. In addition, a letter at the end of the string indicates which transport type was used:

(blank) UDP connection

T	TCP connection
M	Multicast

For example, RTSPT means that the clip was streamed using the RTSP protocol over a TCP connection. The version number indicates the edition of the protocol.

For More Information: See "GET Statements" on page 130.

HTTP Status Code

The HTTP_status_code field holds a return code that uses the HTTP standard error codes. It usually returns 200.

Bytes Sent

The bytes_sent field records the number of bytes transferred to the client by any type of proxy delivery: pass-through, pull-split or cache mode.

Client Information

The [client_info] field describes the version and type of client being used.

RealNetworks Clients

For RealNetworks clients, [client_info] uses the following format:

[*platform_version_client_type_distribution_language_CPU*]

The following information is recorded:

platform	Operating system client software runs on, such as WinNT, Mac, and so on.
version	Operating system version number.
client	Version number of the client software.
type	Type of client software.
distribution	Distribution code of the client software.
language	Language setting in client software.
CPU	Type of processor on which the client is running. If the processor does not have a hardware Floating Point Unit, the string no-FPU is appended to the end of the CPU field with no delimiter.

For example:

```
[WinNT_5.0_6.0.10.714_RealPlayer_RN92PD_en_686]
```

Note: RealAudio Player 1 logs just two fields for [client_info]. They are *platform* and *client*.

Windows Media Player

For Windows Media Player, the [client_info] field records the player version like this:

```
[NSPlayer/7.1.0.3055]
```

QuickTime Player

For QuickTime Player, the client information records the player version and the operating system. For example:

```
[QTS (qtver=5.0.2;os=Windows NT 5.0)]
```

Unknown Clients

If client information can't be gathered because the request came from a client that chose not to send statistics, [UNKNOWN] appears in the [client_info] field.

Client Identifier

For [client_ID], the access log can record an identification number for each media player. This is a globally unique ID. (Helix Universal Proxy typically resides behind a firewall, therefore the proxy does not attempt to gather cookie-based ids for clients.) The following sections explain the possible field entries. The default settings for Helix Universal Proxy and RealNetworks clients record a global ID for each client access attempt. Users can control whether GUIDs are transmitted, however. As well, you can disable the logging of GUIDs through Helix Universal Proxy regardless of client configurations.

For More Information: See "Modifying the Access Log" on page 139 for instructions on turning off client ID logging.

Globally Unique Identifier (GUID) for RealNetworks Client

If a RealNetworks client is configured to send a globally unique ID, it does so. For privacy protection, however, RealOne Player is set by default *not* to send a GUID. Because sending a GUID rests solely at the discretion of each user, users must change their default GUID settings for their GUIDs to appear in the access logs. In RealOne Player, the user command for controlling GUID reporting is **Tools>Preferences> Connection>Internet Settings**.

For More Information: To review RealNetworks' Consumer Software Privacy Statement, see the Web page located at

http://www.realnetworks.com/company/privacy/software.html

Windows Media Player and QuickTime Player IDs

If Windows Media Player and QuickTime Player are configured to send their GUIDs, Helix Universal Proxy records those ID values. If the players do not send GUIDs, Helix Universal Proxy generates an ID for the log. In this case, the same media player may be identified by multiple IDs in the log.

Unknown IDs

When Helix Universal Proxy can't gather an ID because the client does not support GUIDs, empty square brackets—[ ]—appear in the [client_ID] field. If GUID reporting is disabled on the proxy or media player side, the [client_ID] field shows a series of zeroes instead of a unique client identifier:

00000000-0000-0000-0000-000000000000

Statistics Results

The [client_stats_results] field holds connection statistics sent by the client when it finishes playing a clip, as described in "Client Statistics" on page 132. If the client blocks connection statistics, or the statistics cannot be collected, the field appears as [UNKNOWN].

File Information

The following fields hold information about the requested clip:

- The file_size field lists in bytes the amount of media data in the file. This number is less than the total size of the media file because it does not include the file header and other non-media information. For live broadcasts, file_size is always 0.
- The file_time field gives the total length, in seconds, of media stored in the media file. For live broadcasts, file_time is always 0. For SMIL files, this is always 20.
- The sent_time field expresses in seconds the total playing time of the media transmitted to the client.

Resend Information

The resends field lists the number of packets successfully resent because of transmission errors. The failed_resends field gives the number of packets not successfully resent in time to correct transmission errors.

Stream Components

The field [stream_components] is recorded only for RealNetworks media players. It explains the type of material sent, indicated in the following pattern:

```
RealAudio_stream RealVideo_stream Event_stream Image_maps
```

A value of 1 indicates that the clip includes this type of stream. The value 0 indicates that it does not. Thus, a clip that includes RealVideo and RealAudio but no event streams or image maps would appear in the access log as this:

```
1 1 0 0
```

Start Time

The [start_time] field gives the timestamp of when the clip began to stream, according to the Helix Universal Proxy clock. It is identical in format to the timestamp at the beginning of each access record, but does not list the time difference from Coordinated Universal Time. Here is an example:

```
[26/Jun/2002:10:05:14]
```

Server Address

The server_address field lists the IP address of the Helix Universal Server or Helix Universal Proxy that delivered the clip. This may be the origin Helix Universal Server, a Helix Universal Server which is acting as a receiver, or another Helix Universal Proxy which is acting as a proxy receiver.

In proxy cache mode, RTSP requests will show the cache's address (usually 127.0.0.1). To find the address of the origin Helix Universal Server, look in the GET field (see GET Statements on page 130).

Average Bit Rate

The average_bitrate field lists the average bit rate of the clip in bits per second.

Packets Sent

The packets_sent field lists the total number of packets sent to the client.

Presentation ID

The presentation_ID field records a number used by all clips in the same SMIL or Ram presentation. SMIL files are also included in the log, and use the same number as their clips. For example, if the log entries for a SMIL file, a video clip, and a GIF image all list presentation ID 437, you can conclude that the

SMIL presentation consisted of that video and image. Helix Universal Proxy assigns the IDs, which are recorded only with logging style 5, when it transmits the clips.

Proxy Information

The proxy_info field gives information about the type of proxied stream (live or on-demand) and how Helix Universal Proxy delivered the media stream (pass-through, pull-split or cache mode.)

One of the following values is recorded:

Live Pass-Through	The proxied stream was a live clip, and it was sent in pass-through mode.
Live Split	The proxied stream was a live clip, and it was sent using pull splitting.
Demand Pass-Through	The proxied stream was an on-demand clip, and it was sent in pass-through mode.
Demand Cache Hit	The proxied stream was an on-demand clip, and Helix Universal Proxy served it from the media cache.
Unknown	Clip type and delivery were of unknown type.
Accounting Only	Accounting data was sent only, with no media.

GET Statements

The GET statement within an access log record shows the path and file name of each file that Helix Universal Proxy served, as well as the protocol and protocol version used to stream or broadcast the file. The following sections show sample entries for GET statements used with different types of on-demand and live content.

For More Information: To see the GET statement in context, refer to "Logging Style" on page 121.

On-Demand Content

The following table lists the formats in which each type of on-demand content is shown in the GET statements of the access log. For a SMIL presentation, a separate record is generated for the SMIL file and for each file in the presentation. When the logging style is set to 5, you can identify which files

are in the same presentation through the numeric identifier at the end of each access record.

GET Statements for On-Demand Content

Feature	Protocol	Example Statement in Access Log
On-demand streamed content	RTSP	"GET presentation/presentation.rm RTSP/1.0"
	PNA	"GET presentation/presentation.rm PNA/10"
SMIL files (1 record for the SMIL file, one record for each file listed within the SMIL file)	RTSP	"GET presentation/presentation.smi" "GET presentation/presentation.rt" "GET presentation/presentation.rp" "GET presentation/presentation.rm"
Helix Administrator activity	HTTP	"GET admin/index.html HTTP/1.0"
Authenticated on-demand streamed content	RTSP	"GET secure/topsecret.rm RTSP/1.0"
	PNA	"GET secure/topsecret.rm PNA/10"

Live Broadcasts

The following table summarizes the format in which each type of live content is shown in the access log.

Sample GET Statements for Live Content

Feature	Protocol	Example Statement in Access Log
Unicasted, redundant content	RTSP	"GET redundant/live.rm RTSP/1.0"
	PNA	"GET redundant/live.rm PNA/10"
Unicasted content, from RealProducer G2 through 8.5	RTSP	"GET encoder/live.rm RTSP/1.0"
	PNA	"GET encoder/live.rm PNA/10"
Unicasted content, from pre-G2 encoding source	RTSP	"GET live/live.rm RTSP/1.0"
	PNA	"GET live/live.rm PNA/10"
SLTA content	any	same as live unicasted content
Authenticated live streamed content	RTSP	"GET secure/broadcast/live.rm RTSP/1.0"
	PNA	"GET secure/broadcast/live.rm RTSP/1.0"
Multicasting—back-channel	RTSP	"GET encoder/live.rm RTSPM/1.0"
	PNA	"GET encoder/live.rm PNAM/10"

Client Statistics

All logging styles can include client statistics, which are shown in the preceding sections as [client_stats_results]. There are four types of statistics, and the access log can record any combination of them. Each set of statistics is enclosed in square brackets, and begins with a prefix such as Stat1. If you log all four types of statistics, for example, the [client_stats_results] field looks like this:

[Stat1:*statistics_1*][Stat2:*statistics_2*][Stat3:*statistics_3*][Stat4:*statistics_4*]

Note that although other access log fields are separated by spaces, there is no space between the closing square bracket of one statistics type and the opening square bracket of the next statistics type. The following example shows logging style 5 (see page 124) collecting statistics type 1:

```
207.188.7.125 - - [26/Jun/2002:10:11:03 -0700] "GET real9video.rm RTSP/1.0"
200 858636 [WinNT_5.0_6.0.10.714_RealPlayer_RN92PD_en_686]
[00000000-0000-0000-0000-000000000000] [Stat1: 487 2 1 2 0
44_kbps_Stereo_Music_High_Response_-_RA8] 926322 217 205 1 0 124
[Demand Cache Hit]
```

The following sections describe the information gathered by each of the four statistics types. Statistics 1 and 2 report basic information about playback. Statistics 3 provides information about viewer actions. Statistics 4 reports advanced playback information from RealOne Player. The default logging setting gathers statistics 1 and 2. The following table lists the media players and versions that can send the various statistics types.

Media Players and Supported Client Statistics Types

Media Player	Statistics 1	Statistics 2	Statistics 3	Statistics 4
RealPlayer 2 and lower	**yes**	no	no	no
RealPlayer 3 and higher	**yes**	**yes**	no	no
RealPlayer 5 and higher	**yes**	**yes**	**yes**	no
RealOne Player and higher	**yes**	**yes**	**yes**	**yes**
Windows Media Player	**limited**	**limited**	**yes**	no
QuickTime Player	no	no	no	no

Note the following about client statistics:

- Stat1 and Stat2 report codec information only about the audio portion of a clip.

- As noted in the following sections, some statistics are not collected for Windows Media Player. In each case, `0` is typically entered for that statistic.
- Helix Universal Proxy does not record client statistics for QuickTime Player. For each statistics type, `[UNKNOWN]` is logged.
- Users can choose not to send client statistics. On RealOne Player, the command is **Tools>Preferences> Connection>Internet Settings**. If users select this option, `[UNKNOWN]` appears in place of that statistics field.
- The statistics interval, described in "Customizing the Access and Error Logs" on page 139, affects how often statistics are reported.

Statistics Type 1

Statistics type 1 gathers basic information about the success of media clips received by the client. It also tells what codec the client used to decode the audio portion of the clip. The fields are the following:

```
[Stat1: received out_of_order missing early late codec]
```

These fields provide the following information:

`received`	Total number of packets received by the client.
`out_of_order`	Number of packets received by the client out of order. These packets are reordered as the client plays the clip. This information is not recorded for Windows Media Player.
`missing`	Number of packets that the client requested, but that did not arrive.
`early`	Number of requested packets received early by the client. This information is not recorded for Windows Media Player.
`late`	Number of packets received too late by the client. This information is not recorded for Windows Media Player.
`codec`	For Windows Media Player, the names of the audio and video codecs used. For RealNetworks clients, the name of the audio codec used to encode the soundtrack. Possible values for RealNetworks players include: `sipr`—RealAudio version 5 formats `dnet`—RealAudio version 3 formats `28.8`—RealAudio version 2, 28.8 format `lpcJ`—RealAudio version 2, 14.4 format `cook`—RealAudio version 6 format

Statistics Type 2

Statistics type 2 provides details about the success of clip delivery, giving information about bandwidth requests. Resent packets are described in detail. This statistics type identifies which transport type was used to make the connection, and which audio codec played the clip. This set of statistics uses the following format:

```
[Stat2: bandwidth available highest lowest average requested received late
rebuffering transport startup codec]
```

The fields provide the following information:

`bandwidth`	Clip bandwidth in bits per second.
`available`	Average bits per second available to the user while the clip was playing. This information is not recorded for Windows Media Player.
`highest`	Highest time between the client resend packet request and the packet resend arrival, in milliseconds. This information is not recorded for Windows Media Player.
`lowest`	Lowest time between the client resend packet request and the packet resend arrival, in milliseconds. This information is not recorded for Windows Media Player.
`average`	Average time between the client resend packet request and the packet resend arrival, in milliseconds. This information is not recorded for Windows Media Player.
`requested`	Number of resend packets requested by the client.
`received`	Total number of resent packets received by the client.
`late`	Number of resent packets received by the client too late.
`rebuffering`	Rebuffering percentage for the clip.
`transport`	Transport type for the connection. Values are: `0`—UDP `1`—TCP `2`—IP Multicast `3`—PNA over HTTP

`startup`	Time after the media request that the client received the first clip data package, in milliseconds. The data may arrive before the clip starts playing.
`codec`	For Windows Media Player, the names of the audio and video codecs used. For RealNetworks clients, the name of the audio codec used to encoded the soundtrack. Possible values include: `sipr`—RealAudio version 5 formats `dnet`—RealAudio version 3 formats `28.8`—RealAudio version 2, 28.8 format `lpcJ`—RealAudio version 2, 14.4 format `cook`—RealAudio version 6 format

Statistics Type 3

Statistics type 3 provides detailed information about viewer action while playing clips, but not while receiving live broadcasts. It addresses advanced streaming features, notably ads and image maps. For example, you can find out when a viewer clicked on an image map or stopped the clip. Because each user may carry out several actions, the access log file may grow rapidly when you collect these statistics. Be sure to review the log file frequently, or set up log file rolling to keep the logs to a manageable size. This statistics type uses the following format:

```
[Stat3:timestamp|elapsed_time|action|;]
```

Records of activity are separated by a semicolon (;). Thus, the `Stat3` record of a viewer pausing, resuming play, and watching to the clip's end looks like the following:

```
[Stat3:4360|2107|PAUSE|;8401|2107|RESUME|;12608|6321|STOP|;]
```

Timestamp

The initial timestamp field gives the time in milliseconds when the action occurred. It is relative to the connection time of the client. In the preceding example, the first timestamp is `4360`, meaning the action occurred at 4.360 seconds after the client connected.

Elapsed Time

The `elapsed_time` field records how many milliseconds into the clip timeline that the action occurred. In the preceding example, the `PAUSE` action occurs at `2107`, or 2.107 seconds into the clip timeline. Notice that the `RESUME` action

also lists the same elapsed time because this action restarts the clip at the same point where it paused.

Action

The action field records one of several different actions such as `STOP` or `PAUSE`, as described below.

CLICK

Viewer clicked on the image map. Further information includes:

`x-coord`	Horizontal coordinate of the click.
`y-coord`	Vertical coordinate of the click.
`action`	Action that occurred. This is one of the following: `PLAYER="`*`url`*`"`—The URL of a media link the viewer clicked. `URL="`*`url`*`"`—The URL of a browser link the viewer clicked. `SEEK="`*`destination`*`"`—The seek destination point, in milliseconds.

PAUSE

The viewer paused the client.

RESUME

Resume play after a pause, seek, or stop.

SEEK

The seek destination point, in milliseconds.

STOP

End of clip reached.

RECSTART

Media player began recording the clip.

RECEND

Media player stopped recording the clip.

Statistics Type 4

Sent only from RealOne Player, statistics type 4 gathers most of the same information included in statistics type 1 and type 2, adding packet and bandwidth information for each stream. Statistics type 4 reports information for each media stream in the clip, using the following format:

```
[Stat4:stream_number|mime_type|codec|received|lost|resent|average_bandwidth
|current_bandwidth|;...information for next stream...|transport turobplay duration
clip_end]
```

The following is an example type 4 log entry for a RealVideo Clip:

```
[Stat4:2 audio/x-pn-realaudio|44_kbps_Stereo_Music_High_Response_-_RA8
|44100|940|0|0|;video/x-pn-realvideo|N/A|180889|2918|0|0| 1 0|1|0| 90 2]
```

> **Note:** If you turn on statistics type 4 as well as statistics type 1 or 2, RealOne Player reports only statistics type 4. Other media players, however, will report statistics type 1 or 2, but not statistics type 4.

Stream Number

The `stream_number` field indicates how many media streams the clip contains. A video clip might have two streams, for example, one for the audio track and one for the visual track. Following this, information for each stream is reported.

Stream Information

Helix Universal Proxy reports information for each stream. Information ends with a semicolon. For each stream, the following fields are reported:

`mime_type`	MIME type, such as `audio/x-pn-realaudio`.
`codec`	Codec used for the stream, such as `44_kbps_Stereo_Music_High_Response_-_RA8`.
`received`	Number of packets received.
`lost`	Number of packets lost.
`resent`	Number of packets resent.
`average_bandwidth`	Average bandwidth over the course of clip playback in bits per second.
`current_bandwidth`	The bandwidth in bits per second used when the statistics are reported.

Transport

The `transport` field indicates the transport protocol used for the connection. Values are:

`0`	IP Multicast
`1`	UDP

2 TCP

3 HTTP cloaked

TurboPlay

Three turboplay fields indicate the use and results of the RealOne Player TurboPlay feature. The three fields are separated by pipes, as shown here:

```
1|513234|1120
```

The following table lists the possible field values. Values for the second and third field vary depending on whether TurboPlay is on or off, as indicated in the first field.

TurboPlay Field Values

Field 1	Field 2	Field 3
0 (off)	Reason TurboPlay is off: 1—User preference. 2—Available bandwidth below 256 Kbps. 3—SureStream in use. 4—Excess rebuffering. 5—Presentation not enabled for TurboPlay. 6—Server not enabled for TurboPlay. 7—Live presentation not supported.	0 (not used)
1 (on)	Accelerated delivery rate in bits per second requested by TurboPlay.	Average buffering time in milliseconds for start of playback, seeking, and so on.

Duration

The duration field gives the time in milliseconds between the initial client request and the first data packet received by the client.

Clip End

The clip_end field lists the reason the presentation ended. Possible values are:

0 end of presentation reached

1 stop command issued

2 reconnection required

3 redirection

PNR_*n* error code *n* occurred

Information Recorded by Helix Universal Server

If you are also managing a Helix Universal Server, you know that it records similar information about client requests in the server access log as Helix Universal Proxy records in the proxy access log. Additionally, the server access log records extra information (like proxy IP address) when a clip is delivered by either proxy pull splitting or proxy cache.

Helix Universal Server and Helix Universal Proxy access log settings are independent of each other; each installation has independent log files. For example, as someone managing Helix Universal Proxy, you can configure it to record information with Logging Style 0. You can then configure Helix Universal Server to collect all the information of Logging Style 5, resulting in logs that gather different amounts of information.

Customizing the Access and Error Logs

The following sections explain how to modify the logging of access and error records. Logging is turned on by default. You may want to change certain default options, however.

Modifying the Access Log

The access log is preconfigured to gather basic client statistics for media player requests. You may want to change the logging style and client statistics types, as well as set up log file rolling.

➤ To modify access logging:

1. Click **Logging & Monitoring>Access & Error Logging**. Access logging fields are at the top of the page.
2. For **Logging Style**, choose a number from 0 to 5. The default is 5. For information about the logging style, see "Logging Style" on page 121.
3. If you do not wish to collect client identifiers, choose Yes from the **Disable Client GUIDs** pull-down list. This eliminates the collection of client global identifiers. For more information, see "Client Identifier" on page 127.
4. The **Client Stats Interval** setting determines the frequency in seconds that the client reports statistics. A value of 30, for example, means that the client sends statistics, and Helix Universal Proxy creates new log entry,

every 30 seconds. If you set this to 0 (zero), the client sends statistics once when the presentation ends.

5. In the **Client Stats** check boxes, select the types of client statistics that each media player reports. You can choose any combination of statistics, or deselect all boxes to gather no client statistics. The default settings are Type 1 and Type 2. For more information, see "Client Statistics" on page 132.

   Tip: If you gather statistics type 3 or 4, the access log file size will grow rapidly. In this case, be sure to review the log file frequently, or use log file rolling.

6. You can choose to create a new log file at certain intervals, as described in "Log File Rolling" on page 121.
   a. To create a new log file at regular intervals, set the period through the **Log Rolling Frequency** pull-down lists. You can roll the log hourly, daily, weekly, or monthly.
   b. To limit the log file by size, type the maximum number of Megabytes in the **Log Rolling Size** box.

      Tip: Generally, you limit log files by frequency or size. You can select both methods, however, to create log files according to the first limit reached. For example, you can create a new log file whenever the preceding file reaches 10 Megabytes in size, or has recorded 3 days of activity, whichever comes first.

7. The **Proxy Log File** field specifies the log file name and absolute path. The default path is the Logs subdirectory of the Helix Universal Proxy main directory. The default file name of the access log file is proxy.log.

   Note: If **Proxy Log File** is blank, Helix Universal Proxy records access information in a file named, proxy.log, located in the same directory as the Helix Universal Proxy executable file.

8. Click **Apply**.

Modifying the Error Log

Using the error log requires no configuration. You may want to set up log file rolling, though, or specify a different location and name for the error log. For basic information on error log syntax, see "Error Log" on page 120.

➤ To modify the error log:

1. Click **Logging & Monitoring>Access & Error Logging**. Error logging fields are at the bottom of the page.
2. You can choose to generate a new error log file at certain intervals, as described in "Log File Rolling" on page 121.
   a. To create a new log file at regular intervals, set the period through the **Log Rolling Frequency** pull-down lists. You can roll the log hourly, daily, weekly, or monthly.
   b. To limit the log file by size, type the maximum number of Megabytes in the **Log Rolling Size** box.

      Tip: Generally, you limit log files by frequency or size. You can select both methods, however, to create log files according to the first limit reached. For example, you can create a new log file whenever the preceding file reaches 10 Megabytes in size, or has recorded 3 days of activity, whichever comes first.

3. The **Error Log File** field specifies the log file name and absolute path. The default path is the `Logs` subdirectory of the Helix Universal Proxy main directory. The default name of the error log file is `proxyerr.log`.
4. On Windows NT systems, you can send error messages to the Windows Event Viewer. For **NT Event Log Filter**, select the NT error level you want to assign to Helix Universal Proxy error messages.
5. Click **Apply**.

CHAPTER
14
CUSTOM LOGGING

Helix Universal Proxy's custom logging feature allows you to monitor specific types of events and information that occur on Helix Universal Proxy. You can thereby create reports about any type of activity you choose. This chapter explains how to use the custom logging feature, which supplements the main log files described in Chapter 13.

Understanding Custom Logging

Custom logging is a highly flexible feature that allows you to gather the exact information you want, reporting it at any time to different outputs such as the screen or a text file. You can use this feature to gather information about current Helix Universal Proxy client connections, for example. Custom logging is designed to supplement the access and error logging described in Chapter 13, but you may find that custom logging is adequate for all of your logging requirements.

The Helix Universal Proxy Registry

To get information for reports, custom logging relies on information stored in the Helix Universal Proxy registry, which is distinct from the main registry on Windows operating systems. The registry contains information about most aspects of Helix Universal Proxy. Although the registry is an extension of Helix Administrator, there is no link to it from any Helix Administrator page. However, you can display the registry by opening the following URL in a browser:

`http://`*`address:AdminPort`*`/admin/regview.html`

Registry Variables

The Helix Universal Proxy registry stores information in variables such as `LiveConnections.Count`. Each variable reports a specific type of value or setting,

from real-time data on client connections and proxy health, to configuration and license information. When you create a custom logging template, you add variables to your report by selecting them from a pop-up HTML list. Within a report template, variables are always preceded and followed by percent signs, as in `%LiveConnections.Count%`.

Global Variables

Through the variables list, you can also choose global variables, such as the time of day, that are derived from the operating system rather than extracted from the Helix Universal Proxy registry. The following table lists the global variables that you can include in reports.

Global Variables

Variable	Description
`%Date%`	Indicates the current date in the format `MM/DD/YY`.
`%Time%`	Provides the current time of day in the local time zone in the format `HH:MM:SS`.
`%GMTime%`	Displays the current Greenwich Mean Time in the format `HH:MM:SS`.
`%TZDiff%`	Indicates the difference between local time and Greenwich Mean Time. For example, the output for Pacific Standard Time is `-0800`.
`%Hour%`	Displays the current hour by local time zone in the format `HH`.
`%Min%`	Indicates current minute in the format `MM`.
`%Sec%`	Adds the current second in the format `SS`.
`%%`	Creates a percent sign (%).

Template Types

You add the registry variables that you want to track to a report template, which defines how often the selected information is reported, as well as where the report is delivered, such as to a file or to the console. You can use three types of templates:

- Interval

  Interval templates log information at regular intervals, such as every hour. You can define exactly how much time elapses between report output. Interval reports are useful for producing regular status reports about Helix Universal Proxy health, for example.

- Watch

  With a watch template, you can set a watch on a certain variable, or group of variables, generating a report when information changes. A watch template is useful for reporting errors, for example, because a report is generated only when an error occurs.

- Session

  As system activity occurs, Helix Universal Proxy dynamically adds and deletes variables from its registry. When a media player requests a clip, for example, Helix Universal Proxy creates a unique registry entry for that player, storing information such as the player address and the requested URL. A session template reports on this dynamic activity as it happens.

  For More Information: See "Using Session Templates" on page 145 for more information about these templates.

Report Formats

Through the report template, you format a report, adding boilerplate text around selected variables if you wish. For example, you might create an entry like the following:

```
With a total of %LiveConnections.Count% player connections, Helix Universal Proxy
is using %proxy.ClientBW.Total% bits per second of bandwidth.
```

In this example, `%LiveConnections.Count%` and `%proxy.ClientBW.Total%` are variables, and the rest of the text is boilerplate. When Helix Universal Proxy generates the report, it replaces the variable entries with values from its registry. The resulting report looks like this:

```
With a total of 50 player connections, Helix Universal Proxy
is using 2,800,000 bits per second of bandwidth.
```

Using Session Templates

A session template reports on dynamically added and deleted registry variables. Helix Universal Proxy creates registry variables when media players, Helix Universal Servers, and other components connect to it. These variables store information about the component. Using a session template, you can create a report when one of these components connects, disconnects, or both. This lets you record statistics about each media player, for example, such as the player's IP address, its request URL, its bandwidth, and so on.

Choosing a Watch Type

When you create a session template, you select a watch type, which specifies the type of component connection that generates the report. The following table describes the possible values that you can choose.

Watch Types

Watch Type Value	Registry Values Watched
`Client Session [Client.Session]`	Client connections.
`Client Stream [Client.Session.Stream.*]`	Individual media player streams.
`Broadcast Receiver [BroadcastReceiver.Statistics]`	Splitting receivers.
`Broadcast Transmitter [BroadcastDistribution.Statistics]`	Splitting transmitters.
`Broadcast [LiveConnections]`	Live connections.
`Broadcast Archiver [LiveArchiving.Archiver]`	Live broadcast archiving.
`Distributed Licensing[DistributedLicensing. Publishers.Subscribers]`	Distributed licensing.

For example, if you choose `Client Session [Client.Session]` as the watch type, you can generate a report every time a client connects or disconnects. In this case, clients can be media players requesting clips, as well as browsers displaying Helix Administrator HTML pages. In your report, you then choose which registry variables from that client connection you want to log.

> **Tip:** The section "Creating a Client Statistics Log" on page 153 provides an example of how to gather client statistics.

Selecting the Output Format Type

For each session template, you can choose whether to generate the report when the watched component connects, when it disconnects, or both. When you set up the template, you choose an output format from a pull-down list:

`Session Added Output Format`	Generate a report with the specified variables when the watched component connects.
`Session Deleted Output Format`	Generate a report with the specified variables when the component disconnects.

The two output formats allow you to report on different variables when a component session begins, then when it ends. When a client connects, for example, you may want to record several variables, including the client's IP

address, request URL, streaming protocol, transport protocol, and so on. When it disconnects, though, you might want to record just the time and IP address.

Defining Output Methods

The custom logging output methods determine how Helix Universal Proxy publishes the report. There are several options, and you can select multiple delivery methods for each custom log report. Additionally, multiple report templates can write to the same output, such as the same file. Most outputs require configuration. For example, if you send your report to a file and a local TCP port, you specify a file name and a port number.

Console

The `Std Error` (Standard Error) and `Std Out` (Standard Output) options both publish the report to the command line console. No configuration is required.

File

When you select the `File` output method, Helix Universal Proxy publishes the report to a text file, continuously appending new results to the end of the file unless you set up log rolling. You configure the following variables:

`File name`	The log file name. The default location is the main Helix Universal Proxy installation directory. You can specify a relative or absolute path using the syntax appropriate for your operating system.
`Log Rolling Frequency`	How many hours, days, weeks, or months pass before a new log file is created (optional).
`Log Rolling Size`	Maximum size in Megabytes that the log file can become before a new file is created (optional).

Using Log File Rolling

Log rolling is optional, but recommended if you expect to report statistics frequently. If multiple templates write to the same file log file, define log rolling in just one template.

Log Rolling Methods

Generally, you limit log files by frequency or size. You can select both methods, however, to create log files according to the first limit reached. For example,

you can create a new log file whenever the preceding file reaches 10 Megabytes in size, or has recorded 3 days of activity, whichever comes first.

Timestamps

When you implement log rolling, Helix Universal Proxy appends a timestamp to the end of the file name to indicate when the file was created. Suppose that you specify the file name `proxystats.txt`. Your log directory may contain several files with the same base file name, but each with a unique timestamp that looks like this:

```
proxystats.txt20020622134953
```

The timestamp is in the format `YYYYMMDDHHMMSS`, using a 24-hour clock. Hence, the file in the preceding example was created on June 22, 2002, at 1:49.53 P.M.

HTTP Post

With the `HTTP Post` method, Helix Universal Proxy publishes the report to a Common Gateway Interface (CGI) program. You configure the following variables:

`URL`	URL location of the CGI program.
`Port`	Number of the HTTP port on the Web server receiving the log.

TCP Broadcast

The `Outbound TCP` and `Inbound TCP` output destinations let you send the report to an application listening on a specific TCP port. The `Outbound TCP` method publishes the log on a remote computer. For this method, you configure the following variables:

`Destination`	Host name or IP address of the computer that receives the log.
`Port`	Number of an open port on the specified computer.

The `Inbound TCP` method publishes the log on the local computer. You configure the following variable:

`Port`	Number of an open port on the local computer.

UDP Broadcast

The Outbound UDP and Multicast UDP methods publish the report to a UDP socket on a remote computer using unicast or multicast UDP, respectively. You configure the following variables:

Destination	Host name or IP address of the computer where the report should be published. For Multicast UDP, enter a Class D IP multicast address.
Port	Number of an open port on the specified computer.

Pipe and System Log on UNIX

On UNIX operating systems, the Pipe and Syslog methods make the log available to another process, or publish the information to the system log, respectively. For Pipe, you configure the following variable:

Command	Pipe command to the application or script where the information can be post-processed.

For Syslog, you choose one the following priorities, each of which corresponds to an entry type in the UNIX system log:

- LOG_EMERG
- LOG_ALERT
- LOG_CRIT
- LOG_ERR
- LOG_WARNING
- LOG_NOTICE
- LOG_INFO
- LOG_DEBUG

Windows NT Event Log

If you choose NT Event Log, Helix Universal Proxy publishes the report to the event log that corresponds to the priority selected. Each option corresponds to an entry type in the Windows NT Event Log:

- LOG_ERR
- LOG_WARNING

- LOG_INFO

Creating Logging Templates

The following procedure explains how to create a new custom logging template, or modify an existing one. You'll need to be familiar with the information in the preceding sections to set up your custom template. Preconfigured templates are ready to use, but must be turned on. These templates are described in the section "Using the Preconfigured Templates" on page 152.

➤ To create or modify a custom logging template:

1. Click **Logging & Monitoring>Custom Logging**.
2. To create a new template, click the "+" icon in the **Templates** area, and edit the name in the **Template Name** box. This name is for your reference only. To select an existing template, highlight its name in the **Templates** area.
3. In the **Template Type** list box, select `Watch`, `Session`, or `Interval` to set the overall type of template. The option you choose affects other options that appear on the page, as described in Step 7 through Step 9.

   For More Information: See "Template Types" on page 144.

4. From the **Template Status** box, select `On` or `Off` to enable or disable the custom logging report, respectively. An existing template starts or stops reporting as soon as you change its status and click **Apply**.
5. Optionally, you can enter a description in the **Template Description** box. This is for your own reference only, but is highly recommended.
6. You next select one or more output types for the report to determine where Helix Universal Proxy sends the report information:
   a. Select an output type from **Add Output Type** pull-down list.
   b. Optionally, edit the name in the **Output Name** box. This name is for your reference only.
   c. For the selected output type, enter the necessary configuration parameters, as described in "Defining Output Methods" on page 147.
7. If you chose a `Watch` template in Step 3, follow this step. Otherwise, skip to the next step. Click `Property List` in the **Watches** area. In the list that

appears, choose the variable or variables that you want to watch for changes.

> **Note:** Place each watched variable on a separate line in the **Watches** list. Helix Universal Proxy determines which variables to watch by matching the string that appears on each line of the **Watches** list.

The optional minimum and maximum output intervals for the `Watch` template let you generate the report at regular intervals. If you do not define either field, Helix Universal Proxy creates the report only when a watched registry variable changes:

- **Minimum Output Interval**
  This field holds a number in the format `HH:MM:SS` that defines the smallest possible time that must pass between log outputs. Changes to the watched variables are not reported until the minimum interval has elapsed. If you set `00:05:00`, for example, watched variables that change are reported every five minutes. If no watched variable changes its value in five minutes, though, the report is not created until a variable changes, or the maximum interval is reached.
- **Maximum Output Interval**
  This entry contains a number in the format `HH:MM:SS` that defines the longest possible time allowed to pass before the report output is generated. Changes to variables being watched will generate the report output even if the maximum interval has not been reached, however. If you set `01:00:00`, for instance, and no watched variable changes within an hour after the last report, Helix Universal Proxy generates the report when the hour elapses.

8. If you chose `Session` in Step 3, select the appropriate watch type from the **Watch Type** list box. Otherwise, skip to the next step. As described in "Choosing a Watch Type" on page 146, the watch type you select determines which dynamic event triggers the report output.
9. If you chose `Interval` in Step 3, set the appropriate combination of hour, minute, and seconds for the report interval in the **Output Interval** boxes. If you leave a box blank, the setting for that box is considered to be 0.
10. In the **Output Format** area, click **Property List** to pick the variables from the Helix Universal Proxy registry included in the template. If you're setting up a `Session` Template, you can specify up to two output formats,

one for **Session Added Output Format**, and one for **Session Deleted Output Format**.

a. In the property list window, navigate to the variable that you want to include in the template.

b. When you click on a variable, a string identifying that variable appears in the **Output Format** text box. Helix Universal Proxy reports values for variables in the exact order the variables appear in the text box. To organize the order of variables, cut and paste them in the order that you want them to appear in your report.

> **Tip:** A variable added to the **Output Format** text box is surrounded by percentage signs (`%proxy.ClientBW.Total%`). If you reorganize the order of the variables, make sure to include the percent signs that surround each variable name.

c. Optionally, format the report output by adding boilerplate text. Two tags help with formatting the output sting. Use a `\n` tag to move output to a new line. Carriage returns you enter in the box are also recognized as new lines. Use a \t tag to insert a tab.

11. Click **Apply**.

Sample Templates

This section explains how to use the preconfigured templates that come with Helix Universal Proxy. It then provides an example of setting up your own template to log client statistics.

Using the Preconfigured Templates

Helix Universal Proxy comes preconfigured with three templates that illustrate the interval, watch, and session template types. Each template reports output to the console, but is turned off initially. To use a template, you must enable it and, optionally, customize it by changing the output destination or modifying the reporting variables. You can also ignore these templates and create your own. The following sections explain these templates.

Errors Template

The preconfigured `Errors` template is a watch-type template. Whenever Helix Universal Proxy encounters an error, the `Errors` template writes the message to the console. You may want to modify this template to send the output to a file, for example. As well, you can establish minimum and maximum intervals instead of reporting each time an error occurs.

Extended Logging Template

The preconfigured `Extended Logging` template is an example of a session template. It gathers information about client sessions, including media players and Helix Administrator activity, and publishes the report to the console when a client session ends. A single line of the report output looks like this:

```
09:55:28 127.0.0.1 RTSP GET real9video.rm RealMedia Player Version 6.0.9.1349
(win32)
```

Server Stats Template

The preconfigured `Server Stats` template is an example of an interval template. It is designed to send basic proxy statistics to the output console every hour. Optionally, you can modify the variables it reports, write the information to a file, or change its boilerplate text. The report output looks like this:

```
Server Stats (06/17/02 10:33:52)
   Uptime: 1234274 seconds
   CPU Percent Usage: 5
   Players Connected: 32
   Players Connected in the Last 10 Seconds: 2
   Players Connected by Protocol: 0 PNA, 22 RTSP, 10 MMS, 0 HTTP (0 Cloaked)
   Players Connected by Transport: 0 TCP, 32 UDP, 0 MCast
   Total Subscribed Bandwidth Output: 9385984 bps
   Total Actual Bandwidth Output: 9244432 bps
   Average Bandwidth Output Per Player: 293312 bps
   Memory Stats: 14294824 Bytes In Use
```

Creating a Client Statistics Log

This example illustrates how to log information about each client request, including media players requesting clips and browsers requesting Helix Administrator pages. This sample template also logs information when each

client disconnects. In your template, you would set up the following basic parameters:

Template Name:	*any*
Template Type:	Session
Template Status:	on
Template Outputs:	*any*
Watch Type:	Client Session [Client.Session]

Connection Statistics Boilerplate and Variables

For **Session Added Output Format**, you define the report information you want to collect when a client connects. You create a report using boilerplate text and variables chosen from the pop-up property list. Note that \n adds a new line to the report. You can also use \t to insert tabs. Here's an example:

```
\n\n****CLIENT REQUEST****
Date and Time: %Date%, %Hour%:%Min%.%Sec%
**CLIENT INFORMATION**
Type: %Client.*.User-Agent%
Address: %Client.*.Addr%
Total Bandwidth: %Client.*.Bandwidth%
Preferred Language: %Client.*.Language%
**CLIP INFORMATION**
Requested URL: %Client.*.Session.*.PlayerRequestedURL%
Clip Size in Bytes: %Client.*.Session.*.FileSize%
Title: %Client.*.Session.*.FileHeader.Title%
Author: %Client.*.Session.*.FileHeader.Author%
Copyright: %Client.*.Session.*.FileHeader.Copyright%
Stream Count: %Client.*.Session.*.FileHeader.StreamCount%
**TRANSPORT INFORMATION**
Protocol: %Client.*.Protocol%
Port: %Client.*.Port%
UDP used (0=no, 1=yes): %Client.*.IsUDP%
```

Disconnect Statistics Boilerplate and Variables

For **Session Deleted Output Format**, you define the report information you want to collect when a client disconnects. Here's an example:

```
\n\n****CLIENT DISCONNECT****
Date and Time: %Date%, %Hour%:%Min%.%Sec%
Type: %Client.*.User-Agent%
Address: %Client.*.Addr%
Requested URL: %Client.*.Session.*.PlayerRequestedURL%
```

Report Output

Once you've defined your template and applied the changes, Helix Universal Proxy sends the custom logging information to the chosen output each time a client connects or disconnects. The following is an example of a single media player connecting, then disconnecting.

```
****CLIENT REQUEST****
Date and Time: 06/19/02, 14:53.51
**CLIENT INFORMATION**
Type: RealMedia Player Version 6.0.9.1349 (win32)
Address: 207.188.7.125
Total Bandwidth: 57600
Preferred Language: es, *
**CLIP INFORMATION**
Requested URL: rtsp://208.147.89.157:554/video1.rm
Clip Size in Bytes: 2479645
Title: Introductory Video
Author: RealNetworks, Inc.
Copyright: ©2002 RealNetworks, Inc.
Stream Count: 1
**TRANSPORT INFORMATION**
Protocol: RTSP
Port: 7180
UDP used (0=no, 1=yes): 1

****CLIENT DISCONNECT****
Date and Time: 06/19/02, 14:59.15
Type: RealMedia Player Version 6.0.9.1349 (win32)
Address: 207.188.7.125
Requested URL: rtsp://208.147.89.157:554/video1.rm
```

CHAPTER

15

TROUBLESHOOTING

This chapter covers general troubleshooting steps to explore if you experience the unexpected while working with Helix Universal Proxy.

Overview

If you encounter problems when running Helix Universal Proxy, you can narrow down the problem with the following tasks:

- Determine scope of the problem—is the problem with clients connecting to Helix Universal Proxy, or with Helix Universal Proxy connecting to the origin Helix Universal Server?
- Check the error logs—messages in the error log file (or files, if you've set up log file rolling) will direct you to the problem. For instructions on how to interpret the log file formats, see "Error Log" on page 120.

General Troubleshooting Steps

These steps are good ones to check whenever you have trouble with any Helix Universal Proxy features.

Step 1: Make sure Helix Universal Proxy is running.

When you started Helix Universal Proxy, were there any error messages? If so, look up the message in the index of this document.

I can't start Helix Universal Proxy at all.

There are several possible causes of Helix Universal Proxy not starting:

- If you are running Windows NT, Helix Universal Proxy is automatically installed as a service, which means that it runs automatically. If it is installed as a service, and you try to start Helix Universal Proxy using any

other method, it appears not to start. An error message may appear. To find out if it is already running, click **Start>Settings>Control Panel>Administrative Tools>Services** and look for `Helix Proxy` in the list; the word "Started" in the Status field indicates that it's running.

- If you are running UNIX, make sure you are logged on with the correct user name. Helix Universal Proxy requires the use of port 554, and you must be logged on as root in order to access this port. The error message "Could not open port 554" appears on screen when you try to start.
- Your license may have expired, or the license file may have become corrupted. Messages such as the following will indicate this problem.

  "Error - RTSP proxy not licensed for use. Either no license key exists, or the license key present is invalid."

  "Error - PNA proxy not licensed for use. Either no license key exists, or the license key present is invalid."
- The error message "Could not open port 7070" indicates that either other software is using the port, or Helix Universal Proxy could not bind to the necessary address. See the next item for instructions on binding to a particular address.
- You may need to bind Helix Universal Proxy to a specific IP address. This is often the case when you receive the error message "Server not responding properly: Heartbeat check disabled". (Heartbeat check is a self-monitoring feature which ensures that the RTSP port is available.) See "Binding to a Specific IP Address".
- Helix Universal Proxy may be bound to an address that doesn't exist. Using the information in "Binding to a Specific IP Address", either delete the `IPBindings` section, or change it to use the single `0.0.0.0` address.

Binding to a Specific IP Address

To bind to an IP address, open the configuration file in a text editor. If this is a new installation of Helix Universal Proxy, and the configuration file has not been customized, you will need to add the following text to the configuration file. The configuration file is named `rmproxy.cfg`, and is located in the Helix Universal Proxy main directory. Add this text to the end of the file:

```
<List Name="IPBindings">
 <Var Address_01="0.0.0.0"/>
</List>
```

The address `0.0.0.0` binds Helix Universal Proxy to all IP addresses available on this machine. You can substitute the machine's actual address, instead. Note that if you bind to an actual address, you must also bind to the loopback address (`127.0.0.1`).

Determining the IP Address of Your Computer

Use the appropriate method for your operating system:

- **Windows NT**—Click **Start>Run.** In the Run dialog type **cmd**, then click **OK**. At the prompt that appears, type `ipconfig`.
- **UNIX**—Most UNIX platforms will report the IP address if you use the command `ipconfig`.

When I click the Helix Universal Proxy icon, the command window appears briefly but then disappears.

Rather than remaining visible, the window closes if Helix Universal Proxy encounters an error. Use the following steps to find out what the error is:

1. Open a command prompt.
2. Move to the `Bin` directory.
3. Start Helix Universal Proxy by typing

   ```
   Bin\rmproxy rmproxy.cfg
   ```

Helix Universal Proxy will attempt to start, and any error messages will appear on screen. The most frequent causes of this type of problem are an expired license or conflicting port use.

Also, compare your system date to the Issue and Expire date shown on the **About** page of Helix Administrator, and make sure your system date is accurate.

Helix Universal Proxy is running, but many features have stopped working.

If your license files have expired, Helix Universal Proxy runs with minimal settings. See "License File Information" for a list of the features that are always available. Contact RealNetworks or your reseller to purchase an updated license.

Look in the error log for messages.

Helix Universal Proxy's error log (a text file named `proxyerr.log` or `proxyerr`, and located in the Logs directory) may contain a message describing the nature of the problem.

Step 2: Follow the network routing.

If there are any obstacles in the route that RealNetworks system packets take as they move through the network, Helix Universal Proxy may not be able to contact other RealNetworks system components, such as RealPlayers and Helix Universal Servers.

There are two general areas to check:

- Whether Helix Universal Proxy can receive from the origin Helix Universal Server
- Whether a client can receive content from Helix Universal Proxy

Helix Universal Proxy-to-Helix Universal Server Connections

Before investigating any client-to-Helix Universal Proxy issues, be sure the Helix Universal Proxy-to-Helix Universal Server connections are working properly.

Problems may be related to:

- The Helix Universal Server acting as the origin transmitter is no longer broadcasting or is unable to broadcast any clip.
- The administrator of the origin Helix Universal Server has disabled access to all Helix Universal Proxys, or has blocked access of your Helix Universal Proxy in particular.
- The Helix Universal Server acting as the origin transmitter is incorrectly configured for pull splitting.
- A firewall is blocking access. See Chapter 6, "Firewalls" for more information.

On the Helix Universal Proxy machine, use the method described in "Using TELNET to Test Connections" to ensure that the connection between Helix Universal Proxy and Helix Universal Server is clear.

Client-to-Helix Universal Proxy Connections

- Make sure clients are able to connect to Helix Universal Proxy.

- Make certain there aren't any access control rules on Helix Universal Proxy that prohibit the client from receiving any broadcast or stream.
- If Helix Universal Proxy is using multicast to distribute the stream inside the network, look for multicast user list rules that insist that the client receive the broadcast in multicast mode. If the client is not configured for multicast reception, it will not be able to receive the broadcast. See Chapter 8, "Multicasting" for more information.

On the Helix Universal Proxy machine, use the method described in "Using TELNET to Test Connections" to ensure that the connection between the client and Helix Universal Proxy is clear.

Using TELNET to Test Connections

Instructions in this section describe how to use the TELNET program to determine whether a TCP connection exists between two computers. This information is often the first step in figuring out where the problem lies.

If the TELNET program is able to make a successful connection between computers, the problem is not a routing one. Use the troubleshooting guidelines in this chapter to work out a solution.

If the program is not able to make a successful connection, the problem is either a simple configuration issue on the other computer, or it may be a network routing problem.

➤ To use TELNET to test connections between the client and Helix Universal Proxy:

1. Open a TELNET session.
2. At the `telnet>` prompt, type the following command:

   `telnet>open` *`proxy.example.com port`*

   where:

   `proxy.example.com` is the name of the machine on which Helix Universal Proxy is running

   `port` is either of the ports below:

Port Numbers for Client-to-Helix Universal Proxy Connections

Port	Purpose
554	RTSP proxy requests
1090	PNA proxy requests

3. The response indicates your next step.

Telnet Information for Client-to-Helix Universal Proxy Connections

TELNET Response	Significance

`Trying 172.23.16.123...`
`Connected to` *`helixserver.example.com`*`.`
`Escape character is '^'.`
	Helix Universal Proxy is listening on the port you specified. Use troubleshooting steps in this chapter.

`Trying 172.23.16.123...` `telnet: Unable to connect to remote host: Connection refused`	Helix Universal Proxy is not listening on the port specified. Access control rules may be in effect. Or, Helix Universal Proxy may not be binding properly to its addresses.
`Trying 172.23.16.123...` `telnet: Unable to connect to remote host: No route to host`	Helix Universal Proxy's host computer is unreachable. Make sure there is a network connection to the Helix Universal Proxy.
`helixserver.example.com``: Unknown host` or *`helixserver.example.com`*`: Host name lookup failure`	The other computer does not exist, or the host name cannot be resolved by the local DNS server.

➤ To use TELNET to test connections between Helix Universal Proxy and the origin Helix Universal Server:

1. Open a TELNET session.
2. At the `telnet>` prompt, type the following command:

   `telnet>open` *`server.example.com port`*

   where:

   `server.example.com` is the name of the machine on which Helix Universal Server is running

   `port` is the number of the port number you are testing.

Port Numbers for Helix Universal Proxy-to-Helix Universal Server Connections

Port	Purpose
554	Control channel for RTSP requests (data channel also, if TCP was requested)
3030	Data channel for pull splitting requests

(Table Page 1 of 2)

Port Numbers for Helix Universal Proxy-to-Helix Universal Server Connections

Port	Purpose
7070	Control channel for PNA requests (data channel also, if TCP was requested)
7878	Helix Universal Proxy requests for data by the cache to Helix Universal Server (Used with RealSystem Proxy version 8.02 and earlier.)
1755	Helix Universal Proxy listens for MMS requests (for live or on-demand Windows Media clips)

(Table Page 2 of 2)

3. The response indicates your next step.

Telnet Information for Helix Universal Proxy-to-Helix Universal Server Connections

TELNET Response	Significance

`Trying 172.23.16.123...`
`Connected to` *`host.domain`*`.`
`Escape character is '^'.`
	The origin server is listening on the port you specified. Use troubleshooting steps in this chapter.

`Trying 172.23.16.123...` `telnet: Unable to connect to remote host: Connection refused`	The origin Helix Universal Server is not listening on the port specified. Access control rules may be in effect. Or, the origin server may not be binding properly to its addresses.
`Trying 172.23.16.123...` `telnet: Unable to connect to remote host: No route to host`	The origin Helix Universal Server is unreachable.
`host.domain``: Unknown host` or *`host.domain`*`: Host name lookup failure`	Either you are typing an incorrect address, or the origin server does not exist.

Step 3: Ensure that clients are configured correctly.

Be sure that client software is configured to connect to Helix Universal Proxy. Refer to Chapter 5, "Client Configuration".

Step 4: Check remaining areas.

Read further in this chapter for help with specific features.

- Is the Helix Universal Proxy host machine address correctly configured in the network routers? If the client cannot access Helix Universal Proxy over

the network, then you cannot expect media to play. Configuring IP address and routers is a complex issue. Contact a networking specialist for help.

- Is there a firewall between the client and Helix Universal Proxy? Firewalls must be configured to permit media to play through them. See Chapter 6, "Firewalls".
- Is there a parent Helix Universal Proxy in use? If it is misconfigured, all clients may have difficulty receiving streams. Make sure the parent Helix Universal Proxy can make the necessary connections to the Helix Universal Server. See Chapter 7, "Proxy Routing and Redundant Proxies".

Step 5: Work with your system or network administrator.

Others in your organization may have information you need, such as available port numbers, or information on bandwidth restrictions.

Troubleshooting Helix Administrator

How do I figure out which port number to use for Helix Administrator?

1. Using a text editor, open the configuration file, which is named `rmproxy.cfg` and is located in the main Helix Universal Proxy directory, and search the file for `AdminPort`.
2. You will find an entry similar to the following (your port number will be different):

   ```
   <Var AdminPort="7845"/>
   ```

   Make a note of the number.
3. In your Web browser, type the following, substituting your computer's IP address for *address* and the number you found for *AdminPort* in the previous step:

   `http://`*address:AdminPort*`/admin/index.html`
4. Helix Administrator asks you for your user name and password. Type these and click OK.

   Helix Administrator appears.

How do I look up my user name and password?

When you install Helix Universal Proxy, the setup program asks you for a user name and a password. It uses these for Helix Administrator and for any content creators who use G2 encoding software to send material to your Helix Universal Proxy.

If you can't remember your password, you must reinstall Helix Universal Proxy, or contact RealNetworks Technical Support department (see "Contacting RealNetworks Technical Support").

I can't start Helix Administrator.

- Make sure Helix Universal Proxy is running. Helix Administrator cannot start if Helix Universal Proxy is not running.
- You may need to add an IP Bindings section. Refer to "Binding to a Specific IP Address".
- Be certain you are using the name of the machine that's running Helix Universal Proxy in the URL. Do not use a NetBIOS name; use the host name or the IP address, instead.
- Use a newer browser version. The latest version of your Web browser is recommended for browsing Helix Administrator.
- If it was running before, and you have recently created new access control rules, you may have locked yourself out of the administrator. You will need to create a new rule, by editing the configuration file, that allows access to Helix Administrator. See "Access Rule Methods" for an explanation of the necessary rules.

I receive Javascript errors.

Javascript errors are usually due to an older browser version or the wrong version of RealSystem Proxy or Helix Universal Proxy for your operating system. Helix Administrator is designed to run with later versions of your Web browser.

> **For More Information:** Refer to the release notes for the latest information about Web browsers Helix Universal Proxy supports at:
> **http://www.realnetworks.com/resources/contentdelivery/gateway/release_notes.html**

Troubleshooting Pull Splitting

Steps involved in troubleshooting pull splitting fall into two general areas:

- Whether Helix Universal Proxy can receive from the origin Helix Universal Server
- Whether a client can receive a split stream from Helix Universal Proxy

If pull splitting is disabled on the Helix Universal Server acting as the origin transmitter, your Helix Universal Proxy will not be able to serve the clip via pull splitting. It will use pass-through mode for that clip.

Origin Transmitter-to-Helix Universal Proxy Connections

Before investigating any Helix Universal Proxy-to-client issues, be sure the origin transmitter-to-Helix Universal Proxy connections are working properly.

Problems with splitting may be related to:

- The Helix Universal Server acting as the origin transmitter is no longer broadcasting or is unable to broadcast any clip.
- The person administrating Helix Universal Server has disabled pull splitting. This is unlikely, and the feature is enabled by default.
- Helix Universal Server has blocked your Helix Universal Proxy's access.

You can test the connection by connecting a client to the origin transmitter to make sure the clip exists and is being broadcasted; use a client from a machine that is not routed through Helix Universal Proxy.

Helix Universal Proxy-to-Client Connections

Make sure that Helix Universal Proxy can receive a regular unicast from the origin Helix Universal Server. If unicasting is not working, splitting will not work, either.

Make certain there aren't any access control rules on Helix Universal Proxy that prohibit the client from receiving any broadcast or stream.

If Helix Universal Proxy is using multicast to distribute the split broadcast inside the network, look for multicast user list rules that insist that the client receive the broadcast in multicast mode. If the client is not configured for multicast reception, it will not be able to receive the broadcast.

Messages that contain the phrase "bit save" refer to pull splitting.

- "Warning - No split mount point has been defined. Bit save playback will not be supported."
- "Warning - RTSP proxy discarding message from server, data playback occurring from live splitter."
- "Warning - RTSP proxy is detecting redundant splitter challenges."

Troubleshooting Multicasting

Before setting up back-channel multicasting, two conditions must exist:

- Helix Universal Proxy must be licensed for back-channel multicasting
- The network must be set up for back-channel multicasting

If these two conditions have been met, use the following information to troubleshoot this feature.

Steps in troubleshooting back-channel multicasting fall into two areas:

- Running the multicast on Helix Universal Proxy
- Connecting to the multicast with a client

Checking Helix Universal Proxy

The following error messages, appearing in the error log, indicate either that you have configured a back-channel multicast in Helix Administrator with **Multicast Delivery Only** set to `Yes` (`DeliveryOnly=True` in the configuration file):

- "Multicast delivery only"
- "This server is configured to support only multicast connections. Please contact the content provider for more information on listening to this broadcast."

The message "Error in creating Back-channel multicast session. Please increase the AddressRange configuration variable." indicates that Helix Universal Proxy needs more multicast addresses in order to broadcast in back-channel multicast mode. In Helix Administrator, use a larger range in the IP Address Range boxes.

Special Issues with the Configuration File

If you configure back-channel multicast by editing the configuration file directly, you may inadvertently omit required sections. Without a ControlList section, multicasting will not work. Use Helix Administrator to set up the

Client Access Rules.Optionally, add a ControlList section manually to the configuration file. Make sure to use the multicasting tags found in the multicasting chapter of *Helix Universal Proxy Configuration File Reference*.

- "Back-channel multicast is enabled and the control list is empty. No clients will receive multicast. Please add a control list."

If you make changes to the multicasting section of the configuration file, and you make those changes incorrectly, the following error messages may appear in the error log:

- "Warning - Proxy detects that the multicast address range provided is invalid. Check the configuration file."
- "Warning - Proxy cannot determine the IP multicast address range. Check the configuration for proper entry and/or syntax."

Use Helix Administrator to configure multicasting. You may need to check with your network administrator to find out the correct address range to use for your network.

Connecting with the Client

Try to play the clip from the same system on which Helix Universal Proxy is installed.

Problems with multicasting may be related to:

- The network or the client is not multicast-enabled.
- Access control rules prohibit client from receiving any broadcast or stream.
- Multicast user list rules insist that the client receive the broadcast in multicast mode, and the client is not configured for multicast reception.

Troubleshooting Access Control

In addition to the required rules, make sure you have at least three rules, so that you can continue to connect to Helix Administrator, as described in "Access Rule Methods" .

The first rule to create is always the rule that allows you to access Helix Administrator! If you create another rule first, and lock yourself out of Helix Administrator, you will need to edit the configuration file, remove the rule

manually, and then restart Helix Universal Proxy. Refer to the access control chapter of *Helix Universal Proxy Configuration File Reference*.

If you receive the message, "Invalid player IP Address", it is because this Helix Universal Proxy is configured with access rules that prevent clients from certain IP addresses from playing content. The client that tried to request content is excluded via access rules. Access rules are described in Chapter 10, "Access Control".

Troubleshooting Caching

Factors that can affect caching are discussed below.

Cache setting in the Configuration File

If you edit the configuration file directly to configure this feature, you risk accidentally deleting a key section. If you delete the cache mount point information, the following error message appears:

- "Warning - Proxy can not find the cache mount point. Proxy will fall to pass-through."

RealNetworks recommends setting up the cache information using Helix Administrator.

Issues related to Helix Universal Proxy

- Make sure that caching is enabled in Helix Universal Proxy. At the time of installation, caching is turned on by default, however if you've made changes to the configuration, check to see if caching is still turned on. In Helix Administrator, navigate to **Proxy Setting>Cache**. **Enable Caching** should be **Yes**.

Issues related to Helix Universal Server

The configuration of anorigin Helix Universal Server can cause Helix Universal Proxy to deliver files by pass-through instead of from cache, for the following reasons:

- When Helix Universal Server disallows caching of its content.
- When Helix Universal Server encrypts media files, hiding bit information.
- When Helix Universal Server is using a plug-in not included in Helix Universal Proxy's installation. RealNetworks system has an SDK product

that third-party developers can use to create plug-ins that Helix Universal Server and Helix Universal Proxy use to deliver media in custom data formats.

- When Helix Universal Proxy is trying to connect to a legacy RealSystem Server that does not support cache acquisition. (RealSystem Server 5.0 & earlier)
- When Helix Universal Proxy is trying to connect to a RealSystem Server (version 6.0 - 8.0) on the cache port, but is restricted by either a firewall or network issue.

Troubleshooting Proxy Routing

This feature is described in Chapter 7, "Proxy Routing and Redundant Proxies".

Make certain that only the child Helix Universal Proxy has been configured. The parent Helix Universal Proxy receives the child's requests automatically, and requires no settings to do this. If the parent has been configured to send its requests to another Helix Universal Proxy, and no such Helix Universal Proxy is available, clients will display error messages.

If only some requests are being honored, and you have checked that the parent Helix Universal Proxy has not been configured at all, make sure the child's list of rules includes a broad rule that handles all requests not specified in the other rules.

Contacting RealNetworks Technical Support

If you have followed the troubleshooting tips in this chapter and have not been able to solve the problem, check the RealNetworks Knowledge Base for help. The Knowledge Base contains solutions to problems not covered here:

- **http://service.real.com/kb/default.htm**

For technical support with RealNetworks products, please fill out the form at:

- **http://service.real.com/contact/email.htm**

The information you provide in this form will help technical support personnel to give you a prompt response. For general information about RealNetworks' technical support, visit:

- **http://service.real.com/help/call.html**

Information Needed by the RealNetworks Technical Support Department

In addition to asking for a detailed description of the problem you are experiencing, support technicians will want to know the information shown in the following form.

Note: Space for noting information about Helix Universal Server is included for those customers who are also running Helix Universal Server on their networks.

Information About Your Software

	Helix Universal Proxy	Helix Universal Server
Exact server version	9._._._ _ _	9._._._ _ _

For More Information: Refer to "Determining the Helix Universal Proxy Version" for details.

Information About Your System

	Helix Universal Proxy	Helix Universal Server
Operating system	-	-
Processor type and speed	-	-
Available RAM	-	-
Port numbers	-	-
Type of connection to the Internet	-	-
What server processes are present on this system?	-	-
Is the location of cache remote or local?	-	-

Information About Your System

	Helix Universal Proxy	Helix Universal Server
Operating system	-	-
Processor type and speed	-	-
Available RAM	-	-

(Table Page 1 of 2)

Information About Your System (continued)

	Helix Universal Proxy	Helix Universal Server
Port numbers	-	-
Type of connection to the Internet	-	-
What server processes are present on this system?	-	-
Is the location of cache remote or local?‘	-	-

(Table Page 2 of 2)

Information About Other Software

	Helix Universal Proxy	Helix Universal Server
Client software version	-	-
Encoding software version	-	-
Are there any third party plugins being used?	-	-
In as much detail as possible, please explain the problem.	-	-

Information About the Problem

	Helix Universal Proxy	Helix Universal Server
Exact text of error message (if any):	-	-
How are you delivering content—are you streaming on-demand clips or broadcasting live clips?	-	-

(Table Page 1 of 2)

Information About the Problem (continued)

	Helix Universal Proxy	Helix Universal Server
Is the content you're streaming: • live pass-through? • live split? • backchannel multicast • on-demand pass-through • on-demand cache	-	-
To how many clients are you streaming simultaneously, for both live and on-demand streaming?	-	-
If the problem is with a certain feature, when was the last time it worked correctly? What has changed?	-	-
Are there any related problems?	-	-
What features are you using?	-	-
What troubleshooting steps have you already tried?	-	-
What bitrate is the content?	-	-
Are you having difficulties with specific file types?	-	-
Are there any third party plugins being used?	-	-
In as much detail as possible, please explain the problem.	-	-

(Table Page 2 of 2)

Determining the Helix Universal Proxy Version

There are two methods for finding the exact version of Helix Universal Proxy you are running.

➤ To determine the version of Helix Universal Proxy (at a command prompt):

At a command prompt, navigate to the `Bin` directory, and type the following:

```
rmproxy -v
```

The version number appears, in the form `9.x.x.xxx`, where *x* varies according to your operating system.

➤ To determine the version of Helix Universal Proxy (through Helix Administrator):

In Helix Administrator, click **About**.

A new browser window appears, with information about your proxy.

The version number can vary according to the operating system you use. If you are contacting the RealNetworks Technical Support department for assistance, it is important that they know the exact version you have.

> **Note:** If you are also using a Helix Universal Server, these same steps can be used to determine the version of Helix Universal Server.

APPENDIX

A

CONFIGURATION FILE

When you start Helix Universal Proxy, it reads its default configuration file, `rmproxy.cfg`. When you change Helix Universal Proxy configuration information, Helix Administrator updates the configuration file automatically. This appendix provides general information, and describes the structure of the configuration file.

Configuration File Basics

The following sections provide background information about configuration files that you may find useful.

Alternate Configuration Files

As the sections on starting Helix Universal Proxy explain, you can specify a configuration file other than `rmproxy.cfg` at startup. This might be a file that you have manually edited, using a copy of `rmproxy.cfg` as a starting point. For instructions on using alternate files, see "Starting Helix Universal Proxy" on page 28, or "Starting on UNIX" on page 29.

Security

Be sure to store the configuration file where only authorized users can make changes to it. The default location is Helix Universal Proxy's main installation directory.

Backup Configuration File

The Helix Universal Proxy installation directory also contains a backup copy of the configuration file named `default.cfg`. This is a mirror image of the default `rmproxy.cfg` file that was created during installation. You can restore your configuration file from the backup if you make changes that you want to undo, or if you accidentally delete the main copy.

Configuration File Text Editing Guidelines

You can change the Helix Universal Proxy settings by opening the configuration file with any text editor. You can also add variables that aren't included in the initial file. Refer to *Helix Universal Proxy Configuration File Reference* to learn more about the variables you can use with Helix Universal Proxy.

In addition, third-party plug-ins may require their own parameters and variables. Use a text editor to add them to the configuration file.

To make changes to existing settings in this file is simple; this section provides guidance. If, however, you plan to add new sections, you will need to understand the syntax of the entire file. The file is organized into sections. This is not strictly necessary, but helps with clarity. The structure of the configuration file is described in detail in the section "Configuration File Syntax" on page 177.

> **Tip:** It is recommended that you first use Helix Administrator to make changes, and then examine the configuration file to learn how changes are made. Noticing how lists are created and changed will be especially instructive.

Helix Administrator Exit

Helix Administrator shows the configuration file settings of the Helix Universal Proxy configuration file in use. Therefore, you should exit Helix Administrator before opening the configuration file with a text editor or unexpected changes may result.

Multiple Proxies

The default name of the configuration file is `rmproxy.cfg`, but if you have multiple proxies you may want to rename the files so as to easily identify which proxy you're working with.

Correct Syntax

When you edit the configuration file manually, be sure to use correct syntax, because Helix Universal Proxy looks for exact spellings and correct use of angle brackets. Helix Universal Proxy does not display messages related to syntax errors; instead, it will ignore those settings it does not understand.

Helix Universal Proxy Restart

Always restart Helix Universal Proxy after changing any settings in the configuration file with a text editor.

Configuration File Syntax

The configuration file is a text-only file formatted with tags that are based on XML (eXtensible Markup Language). This provides a high degree of flexibility, enabling third parties to extend Helix Universal Proxy's functionality. Using third-party additions to Helix Universal Proxy may require you to edit the configuration file by hand to enable the features.

The configuration file is constructed entirely of tags. There are four types of tags in this file: the XML declaration tag, optional comment tags, list tags, and variable tags.

Of these four types, only two make up the instructions to Helix Universal Proxy: lists and variables. Lists are used for instructions that have several parts, such as the MIME types or the multicast instructions. A list tag is followed by one or more list tags or variable tags.

All values for lists and variables are enclosed in double quotation marks.

> **For More Information:** Refer to *Helix Universal Proxy Configuration File Reference* to learn more about the contents of the configuration file.

XML Declaration Tag

The XML declaration tag indicates which version of XML is in use. Helix Universal Proxy uses XML version 1.0. The declaration tag looks like this:

```
<?XML Version="1.0" ?>
```

Comment Tags

Comment tags are used in the configuration file to identify the functions of tags, but the comments aren't required. XML comment tags are just like those in HTML: they begin with <!-- and end with -->. Helix Universal Proxy ignores these tags; they are for your benefit.

For example, this comment tag lets the administrator know that the parameters after it refer to the path settings:

```
<!-- P A T H S -->
```

> **Tip:** To disable a feature, convert the feature's tag or tags to a comment. Rather than converting each tag to a comment, edit only the feature's first opening tag and last closing tag.

Do not nest comment tags within other comment tags.

List Tags

The list tag uses the following syntax:

```
<List Name="name">
...
</List>
```

where *name* is the list title. Using the correct capitalization for *name* is important.

Other lists or variables follow the list. The `</List>` tag signifies the end of the list. If other lists are inside the original list, they must also have closing `</List>` tags. The `ProxyAlternates` list is an example of a list that contains other lists.

> **Tip:** Indenting list items is not required, but is recommended for clarity.

Variable Tags

Variable tags use the following syntax:

```
<Var name="value"/>
```

where *name* is the variable title, and *value* is a string or a number, depending on the variable. Capitalization for both *name* and *value* is important.

Unlike lists, variables do not have a closing tag; instead, a forward slash mark (/) appears before the closing angle bracket (>).

> **Tip:** If you've restarted Helix Universal Proxy and it's not responding to a change you've made to a variable, make sure the variable has a closing forward slash mark, and that there is no space between them.

Variables can be independent elements (such as `LogPath`) or they may appear inside a list. When variables appear within a list, their meaning is determined

by the value of the list name, although they may be apparently identical in syntax to variables that are not inside lists. If there are multiple variables within a list that do similar things, their names must be unique. For example, the `Extension` variables within each `MIMETypes` list must have different names; this is accomplished by adding a number to the end of each (`Extension_01`, `Extension_02`, and so on).

APPENDIX

B

ADDRESS SPACE BIT MASKS

In the multicasting and access control features of Helix Universal Proxy, you can identify a range of IP addresses by assigning a bit mask to an IP address. Helix Universal Proxy interprets the bit mask as a single, contiguous block of address spaces. This appendix describes how to create a bit mask for the purpose of identifying a range of IP addresses.

Understanding Basic IP Address Construction

To understand how bit masks work, it is helpful to review the basic concepts for constructing an IP address. Each IP address is 32 bits, divided into four 8-bit octets. Each bit in an octet is assigned a value between 128 and 1, from left to right. To indicate whether a value is in use, the bit is set to 1. The sum of all bit values for each octet determines the octet's dotted decimal value. The following defines values for each bit in an octet:

	Bit 1	**Bit 2**	**Bit 3**	**Bit 4**	**Bit 5**	**Bit 6**	**Bit 7**	**Bit 8**
Bit Value:	128	64	32	16	8	4	2	1

It is possible to make any number between 0 and 255 simply by indicating whether each bit in an octet is set to 1 or 0. For example, both of the following expressions indicate the same IP address:

dotted decimal:	`192.0.1.2`
32-bit binary equivalent:	`11000000 00000000 00000001 00000010`

Using a Bit Mask to Identify an Address Space

To indicate a range of IP addresses, you must first identify the *lowest* IP address in your range, and then indicate the number of bits that are identical between

that address and the highest IP address in the range. Consider the range of IP addresses 192.0.1.255 to 192.0.1.0.

These two addresses indicate a range of 256 possible address (in practice only 254, because the all-zero and all-one addresses are reserved). Between the two indicated addresses, 192.0.1.0 is the lowest in the range, and the first three octets (the first 24 bits) are exactly the same for both addresses. Consider the following addresses and the bit mask expressed in binary.

Addresses and Bit Mask

Address and Mask	Dotted Decimal	32-Bit Binary Equivalent
Highest Address	192.0.1.255	11000000 00000000 00000001 11111111
Lowest Address	192.0.1.0	11000000 00000000 00000001 00000000
Bit Mask	24 Bits	11111111 11111111 11111111 00000000

Notice that the first 24 bits in the highest and lowest addresses are exactly the same. The same would be true if you had used an address with any decimal number (0-255) in the last octet. The bit mask uses 1's to indicate bits to be evaluated, and 0's to indicate bits to be masked. Thus, assigning a bit mask of 255.255.255.0 to the lowest IP address in the range indicates an address space of 256 possible IP addresses.

Slash Notation

In the preceding table, the bit mask appears in both its dotted decimal and 32-Bit binary form. However, this same address space can also be articulated with *slash notation* like this:

192.0.1.0/24

Slash notation uses the lowest IP address in the range, followed by a slash and a number that indicates how many bits should be evaluated. This is helpful to understand because in Helix Universal Proxy you indicate a bit mask in a similar manner. You select the number of bits—from 0 bits through 32 bits—from a pull-down list.

Address Space Size

The size of the address space is determined by the number of bits included in the bit mask. The fewer bits used, the more addresses that are included in the address space. An 8-bit mask includes 2^{24} power addresses, while a 24-bit mask includes only 2^{8} power addresses.

Bit Boundaries

Bit boundaries also affect which address can be included in an address space. To understand how bit boundaries work, recall that each octet includes 8 bits, and that each bit has an assigned value. Ranges correspond to the value of each bit in an octet. Further, these ranges cannot cross bit boundaries. Consider the following addresses:

Bit Boundary with an Inappropriate Mask

Address and Mask	Dotted Decimal	32-Bit Binary Equivalent
Highest Address	192.0.0.2	11000000 00000000 00000000 00000010
Lowest Address	192.0.0.1	11000000 00000000 00000000 00000001
Bit Mask	31 Bits	11111111 11111111 11111111 11111110

Although there are only two consecutive addresses in the range shown in the preceding table, you cannot create a range of two with these addresses, because bit 31 is different for each address. This is a bit boundary. To create a range for these addresses, use the sixth bit in the fourth octet, or a bit mask of 30. Note, though, that by using 30 bits, you also end up including more addresses:

Bit Boundary with an Appropriate Mask

Address and Mask	Dotted Decimal	32-Bit Binary Equivalent
Highest Address	192.0.1.3	11000000 00000000 00000001 00000011
	192.0.1.2	11000000 00000000 00000001 00000010
	192.0.1.1	11000000 00000000 00000001 00000001
Lowest Address	192.0.1.0	11000000 00000000 00000001 00000000
Bit Mask	30 Bits	11111111 11111111 11111111 11111100

Determining Bit Boundaries

The chart below identifies every literal bit range available. Look up the bit for the octet you are working with in the **Bit** column on the left. Then use the corresponding **Literal Bit Range** column to look up the decimal values available for each range.

For example, the problem described above arose from attempting to use bit 7 in the fourth octet (Bit 31). However, in row 7 of the table below, no range includes decimal 1 through 2. For a range that works, you need to use the

sixth bit in the fourth octet (Bit 30). Notice that in row 6, there is a decimal range that includes 1 through 2 (range 0-3).

Literal Bit Ranges

Bit	Literal Bit Ranges
1	Ranges of 0-127; or 128-255
2	Ranges of 0-63; 64-127; 128-191; or 192-255
3	Ranges of 0-31; 32-63; 64-95; 96-127; 128-159; 160-191; 192-223; 224-255
4	Ranges of 0-15; 16-31; 32-47; 48-63; 64-79; 80-95; 96-111; 112-127; 128-143; 144-159; 160-175; 176-191; 192-207; 208-223; 224-239; 240-255
5	Ranges of 0-7; 8-15; 16-23; 24-31; 32-39; 40-47; 48-55; 56-63; 64-71; 72-79; 80-87; 88-95; 96-103; 104-111; 112-119; 120-127; 128-135; 136-143; 144-151; 152-159; 160-167; 168-175; 176-183; 184-191; 192-199; 200-207; 208-215; 216-223; 224-231; 232-239; 240-247; 248-255
6	Ranges of 0-3; 4-7; 8-11; 12-15; 16-19; 20-23; 24-27; 28-31; 32-35; 36-39; 40-43; 44-47; 48-51; 52-55; 56-59; 60-63; 64-67; 68-71; 72-75; 76-79; 80-83; 84-87; 88-91; 92-95; 96-99; 100-103; 104-107; 108-111; 112-115; 116-119; 120-123; 124-127; 128-131; 132-135; 136-139; 140-143; 144-147; 148-151; 152-155; 156-159; 160-163; 164-167; 168-171; 172-175; 176-179; 180-183; 184-187; 188-191; 192-195; 196-199; 200-203; 204-207; 208-211; 212-215; 216-219; 220-223; 224-227; 228-231; 232-235; 236-239; 240-243; 244-247; 248-251; 252-255
7	Ranges of 0-1; 2-3; 4-5; 6-7; 8-9; 10-11; 12-13; 14-15; 16-17; 18-19; 20-21; 22-23; 24-25; 26-27; 28-29; 30-31; 32-33; 34-35; 36-37; 38-39; 40-41; 42-43; 44-45; 46-47; 48-49; 50-51; 52-53; 54-55; 56-57; 58-59; 60-61; 62-63; 64-65; 66-67; 68-69; 70-71; 72-73; 74-75; 76-77; 78-79; 80-81; 82-83; 84-85; 86-87; 88-89; 90-91; 92-93; 94-95; 96- 97; 98-99; 100-101; 102-103; 104-105; 106-107; 108-109; 110-111; 112-113; 114-115; 116-117; 118-119; 120-121; 122-123; 124-125; 126-127; 128-129; 130-131; 132-133; 134-135; 136-137; 138-139; 140-141; 142-143; 144-145; 146-147; 148-149; 150-151; 152-153; 154-155; 156-157; 158-159; 160-161; 162-163; 164-165; 166-167; 168-169; 170-171; 172-173; 174-175; 176-177; 178-179; 180-181; 182-183; 184-185; 186-187; 188-189; 190-191; 192-193; 194-195; 196-197; 198-199 200-201; 202-203; 204-205; 206-207; 208-209; 210-211; 212-213; 214-215; 216-217; 218-219; 220-221; 222-223; 224-225; 226-227; 228-229; 230-231; 232-233; 234-235; 236-237; 238-239; 240-241; 242-243; 244-245; 246-247; 248-249; 250-251; 252-253; 254-255
8	Only an exact match is possible.

Working with 0-Bit and 32-Bit Masks

There are two masks that create somewhat special cases: 0-Bits and 32-Bits. When an IP address has a 32-Bit mask, it creates a literal range of 1. For example, consider the following address and 32-Bit mask:

```
192.0.1.1 /32
```

When Helix Universal Proxy evaluates incoming IP addresses against this IP address, there is only one possible match: 192.0.1.1. For a match, the incoming address must match all 32-Bits in the original address.

Just as there is only one possible match for addresses with a 32-Bit mask, the opposite is true for addresses with a 0-Bit mask. An IP address with a 0-bit mask essentially tells Helix Universal Proxy to match any addresses. Although not required, you should also enter an origin address of all zeros, like so:

```
0.0.0.0 /0
```

This works because Helix Universal Proxy uses a Boolean *and* operation to evaluate incoming addresses. In this type of algorithm, anything and zero equals zero, so all incoming addresses end up equal to the all-zero address entered as the origin address.

APPENDIX

C

AUTHENTICATION DATA STORAGE

This chapter describes the data storage methods which can be used with the authentication feature.

Understanding Authentication Data

To authenticate visitors, the Helix Universal Proxy stores user IDs and passwords. When a client makes a request for media, Helix Universal Proxy looks up this information to see whether the client or visitor is authorized. The information can be stored in either a series of text files or in a database. Templates for common databases are installed during installation.

This section describes the methods for storing user name and password data. Templates for common databases are created during installation, that correspond to the database methods listed in "Setting up Databases" on page 106.

- **Text file storage**—this method uses a combination of directory structure and text files to achieve a sensible data storage method. It is the default method. See "Using Text Files for Authentication Data" on page 188 for details.
- **Database templates**—the supplied templates use a similar structure to the text file method, in more familiar database formats. Refer to "Using a Database for Authentication Data" on page 190 for more information.

Using Text Files for Authentication Data

The default configuration uses the text file storage method to provide storage for both default realms.

The following directories contain the text files which store data. The center letter indicates the authentication protocol: r is for RN5, b is for Basic.

Supplied Data Storage Directories

Directory Name	Data Storage for the following type of information
adm_b_db	Helix Administrator User Authentication
con_r_db	Connection Authentication

The contents of the directories are given in the table below.:

Text File Storage Directory Structure

Directory	Contents	File or Directory Description
Main directory (con_r_db or adm_b_db)	ppvbasic.txt	The text file indicates to Helix Universal Proxy that this is the storage area for the list of authenticated names.
users	(initially blank)	Files in this directory list the clips and permission types.
logs	access.txt	See below for a description.
guid	(initially blank)	For player validation, files contain GUIDS to identify individual players.
redirect	(initially blank)	For player validation, files contain an URL to which to send the client if redirection is necessary.

When Helix Universal Proxy creates the file structure, it creates the ppvbasic.txt file. The second and subsequent times you start the Helix Universal Proxy, the program looks for this file. If the file does not exist, it recreates the directory structure.

> **Warning!** Do not delete the ppvbasic.txt file! If you delete the ppvbasic.txt file, Helix Universal Proxy will rewrite the directories and will erase their prior content.

Users Directory

The files in this directory are named *username*, where *username* is the user name. This directory contains one file per registered user.

The first line of each file has the following format:

password;uuid;uuid_writeable

where:

password	When user authentication is in use, this stores the password. Otherwise shows an asterisk (*). Note: Passwords are encrypted. To change them manually, see "Changing RealSystem 5.0 Authentication Passwords".
uuid	In player validation, stores playerID. In user authentication, an asterisk (*) appears in this field.
uuid_writeable	A flag set and used by Helix Universal Proxy: 0 playerID is in database 1 record created, but playerID is not yet registered

Note: If you manually edit the files, be sure that any blank (or unused) fields use an asterisk (*) as a placeholder. Do not use a space for a placeholder.

Logs Directory

This directory contains access.txt, which is not created until authentication is enabled and the first user connects to Helix Universal Proxy.

Access.txt

Each line of access.txt describes the result of an attempt to view a clip. Syntax of this file:

status;userid;uuid;ip;url;access_type;permission_on;start_time;end_time;total_time; why_disconnect

where:

status	Result of user's attempt to connect: 0 access to clip granted 1 denied
userid	Unique name of up to 50 characters.
uuid	Stores playerID.
ip	IP address from which user is attempting to connect
url	Secured clip user is attempted to access.
permission_type	Event value.
permission_on	Always 0.
start_time	Time/date clip started playing.

end_time	Time/date clip stopped playing.
total_time	Total time clip played.
why_disconnect	Reasons for disconnection: 0 client disconnected voluntarily 1 server access expired

Using a Database for Authentication Data

This section describes the structure of the ODBC, MS SQL and mSQL database templates included with Helix Universal Proxy.

To set up the database on Windows and UNIX, see "Setting Up Other Types of Data Storage".

The database templates include these tables:

- **Users table**—Lists who is registered and with what access.
- **Access_log table**—Used by this feature.

Users Table

Gives the list of user names and passwords.

Users Table

Field	Description
userid	User name of up to 50 characters. Ties to permissions table.
password	In user authentication, this stores the password. Otherwise blank. Note: Passwords are encrypted. To change them manually, see "Changing RealSystem 5.0 Authentication Passwords".
uuid	In player validation, stores clientID. In user authentication, an asterisk (*) appears in this field.
uuid_writeable	A flag set and used by Helix Universal Proxy: 0 clientID is in the database 1 the record has been created but the clientID is not yet registered with Helix Universal Proxy.

Access_log Table

Shows which restricted sites have been accessed.

Access_log Table

Field	Description
status	Result of user's attempt to connect: 0 access to clip granted 1 denied
userid	Unique name of up to 50 characters.
uuid	Stores player ID.
ip	IP address from which user is attempting to connect.
url	Secured clip user is attempted to access.
permission_type	Event value.
permission_on	This field is always 0.
start_time	Time/date clip started playing.
end_time	Time/date clip stopped playing.
total_time	Total time clip played.
why_disconnect	Reason for disconnection: 0 client disconnected voluntarily 1 server access expired

Setting Up Other Types of Data Storage

➤ To set up your Windows computer for ODBC compliance:

1. On the **Start** menu, point to **Settings**, and click **Control Panel**.
2. Under **Administrative Tools**, double-click **Data Source (ODBC).**
3. On the **System DSN** tab, click **Add**.
4. Select your ODBC driver from the list of drivers and click **Finish**.
5. In the **ODBC SQL Server Setup** dialog box, type the data source name. Click **Select**.
6. Type or browse for the path to your database file and click **OK**.
7. Click **OK** to exit the ODBC Data Source Administrator.

> **Note:** You must now tell Helix Universal Proxy where to find your database. Refer to "Setting up Databases".

➤ To set up the supplied mSQL database on UNIX:

1. Move to the directory where mSQL is located.
2. At a command line, start mSQL by typing the following:

   `./msql2d &`

   where

   `&` starts mSQL in the backround.
3. Create the database by typing the following:

   `./msqladmin create` *`databasename`*

   > **Note:** Whatever you type for *`databasename`* needs to match the database cited in **Security>User Databases**.

4. Create the tables using the sample database template by typing the following:

   `./bin/msql -h` *`localhost databasename`* `<` *`authdemo`*

   where:

   `authdemo` is `/Database/msql/authdemo.db`, in Helix Universal Proxy's installation directory.

   > **Note:** Be sure to include the less-than sign (<).

INDEX